Malaysian Public Sector Management Of Information & Communications Technology Security Handbook (MyMIS)

MyMIS adalah satu panduan yang disediakan bagi membantu membangunkan infrastruktur keselamatan ICT. Ia meliputi pengurusan keselamatan, isu operasi, isu teknikal dan implikasi perundangan. Selain daripada itu, ia juga menyediakan template, beberapa contoh senarai semak dan peraturan - peraturan yang boleh dijadikan sebagai panduan dalam membantu membangunkan dasar keselamatan ICT sesebuah organisasi ke tahap yang kukuh. MyMIS mengandungi 5 (lima) bab seperti berikut:

Bab pertama – bab pengenalan yang menerangkan tentang sasaran pembaca dan ruang lingkup garis panduan berlandaskan beberapa standard yang telah dikemukakan dalam keselamatan ICT.

Bab kedua – bab pengurusan keselamatan yang menekankan elemen-elemen penting yang perlu dipertimbangkan oleh sektor awam dalam melindungi sistem ICT organisasi masing-masing. Bagi mencapai maklamat tersebut, pihak pengurusan mestilah mempunyai pengetahuan yang secukupnya dan memberi komitmen yang tinggi dalam menyediakan penyelesaian yang sesuai dan tepat berkenaan isu - isu keselamatan ICT.

Bab ketiga – bab operasi asas yang menerangkan cara pemakaian keselamatan ICT dalam sektor awam yang dihubungkaitkan dengan klasifikasi maklumat, peranan dan tanggungjawab, faktor-faktor kemanusiaan, kemudahan elektronik, pengurusan media, pengurusan penyimpanan, pengendalian bencana, perancangan kontingensi dan perlindungan fizikal dan persekitaran.

Bab keempat – bab operasi teknikal menerangkan keselamatan dari segi teknikal yang meliputi penggunaan keselamatan ICT ke atas peralatan dan perisian komunikasi, sistem operasi, perisian atau aplikasi dan lain-lain-lain peralatan yang berkaitan.

Bab kelima – bab perundangan pula menyentuh tentang undang-undang siber dan undang-undang lain yang berkaitan. Bab ini juga menerangkan kesalahan-kesalahan jenayah komputer dan implikasi perundangannya.

MyMIS telah dibentang dalam mesyuarat Jawatankuasa IT dan Internet Kerajaan (JITIK) pada 17hb Mei 2001. Dalam mesyuarat tersebut, JITIK setuju dokumen MyMIS diterimapakai sebagai rujukan dan garis panduan keselamatan ICT Sektor Awam.

Chapter 1 INTRODUCTION

1.1 General

Definition

“Public Sector ICT Security can be defined as the process of ensuring business continuity and services provision free from unacceptable risk. It also seek to minimize disruptions or damage by preventing and minimizing security incidents” – Public Sector ICT Security Policy (Appendix A).

Security of information within the government’s ICT system is a major concern

The security of information within the Government of Malaysia’s Information and Communications Technology (ICT) system is a subject of major concern. Threats such as impersonation, malicious code, misuse of data, easily available penetration tools, powerful analytical techniques contribute in whole or in part to the necessity of providing adequate protection to public sector ICT assets. These threats if left unchecked, will result in painful explaination at the very minimum or untold damage to the country. Apart from incurring financial losses, both in terms of resources and unavailable services, these threats severely jeopardises the confidentiality, integrity and availability of official government information and in the end may be of detriment to the country. The hardest thing to comprehend is that an attack can be easily mounted by anyone from anywhere courtesy of the information superhighway and the misused concept of global instantaneous information sharing. Some examples of common threats are listed in Appendix B.

Need for effective Public Sector ICT Security management

Over the years, government agencies have been religiously collecting vast amount of information. It is in the early 70’s that these information have been deposited into digital format and since then, these repositories have unknowingly become exposed because of the invaluable information they keep and now in a format easily manipulated without stringent audit trail. The government realises this and that the government is also aware that there is an urgent need to secure the vast information resource through effective management of the security of ICT systems. In this regard, efforts are being made to ensure Public Sector ICT Security management achieve and maintain a high level of confidentiality, integrity and availability.

A comprehensive approach to ICT Security processes is required

A comprehensive approach is required in planning, developing, operating and maintaining the government’s ICT security processes. The ICT security measures need to be incorporated early, in the requirement specification and design of the ICT system, before the implementation stage to ensure a cost-effective and comprehensive system. The main steps include:

(a) assessing the current security strengths and vulnerabilities;

(b) developing ICT security policies, standards and processes;

(c) designing and developing a customised security architecture; and

(d) evaluating and selecting the best security system for the organisation.

Copyright MAMPU

The ICT security process must cover various aspects in achieving a secure enviroment

The ICT security process must cover all aspects of operation, including mechanisms used by hardware and software systems, networks, databases and other related systems and facilities. The goal is to achieve a secure working environment for employees and other persons working at or visiting the government's facilities as well as to help establish processes to ensure the protection of information.

ICT security processes should mirror management's direction

The ICT security process should mirror the management's direction in relation to:

(a) overall organisational policy;

(b) organisational roles and responsibilities;

(c) personnel;

(d) government's asset classification and control;

(e) physical security;

(f) system access controls;

(g) network and computer management;

(h) application development and maintenance;

(i) business continuity;

(j) compliance to standards as well as legal and statutory requirements;

(k) classification and protection of information media;

(l) employee awareness programmes; and

(m) incident reporting and response.

1.2 Standards Framework

This handbook provides guidelines on ICT security based on international standards

This handbook provides essential guidelines to government employees on the ICT security process in the public sector. It is based mainly on two standards i.e. the MS ISO/IEC 13335 (Part 1 - 3) and the BS 7799 (Part 1 and 2). It also makes references to the Canadian Handbook on Information Technology Security, German IT Baseline Protection Manual and other related ISO standards.

Various levels of details of standards can be viewed in the model depicted in Figure 1.1. In comparison to other standards and documents of ICT security management particularly to their level of detail, this handbook can be positioned along with the BS 7799, the Canadian MG-9 and the American National Institute of Science and Technology (NIST). This is warranted by the fact that this handbook is jurisdictional and specific to the Malaysian public sector.

Description of model (Figure 1.1)

In the model, the areas and level of details of these standards varies between each standard. Level 1, 2, 3 and 4 represent the Guidelines for the Management of IT Security (GMITS) or ISO/IEC 13335. It indicates the depth of knowledge required to understand the respective level. As an example, a Level 1 document needs no prior knowledge on ICT security management while a Level 2 document needs at least some understanding of the previous level.

Level 1 to level 4 of the model

The model progresses from Level 1 'Concepts and Models' to Level 2 'Managing and Planning IT', Level 3 'Techniques for the Management of IT' before detailing 'Selection of Safeguards, Management Guidance on Network and Guidelines for the Management of Trusted Third Parties' in Level 4.

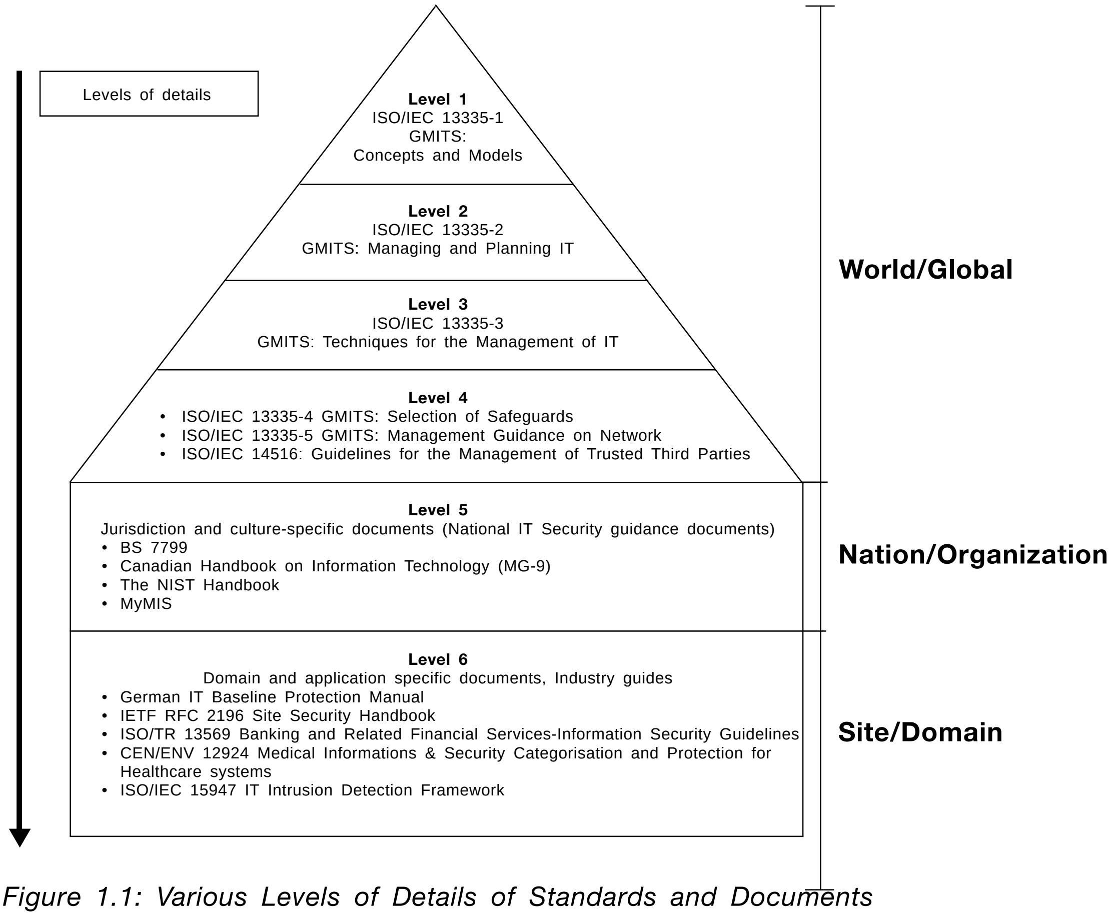

Levels of details
Level 1
ISO/IEC 13335-1
GMITS:
Concepts and Models
Level 2
ISO/IEC 13335-2
GMITS: Managing and Planning IT
Level 3
ISO/IEC 13335-3
GMITS: Techniques for the Management of IT
Level 4
• ISO/IEC 13335-4 GMITS: Selection of Safeguards
• ISO/IEC 13335-5 GMITS: Management Guidance on Network
• ISO/IEC 14516: Guidelines for the Management of Trusted Third Parties
Level 5
Jurisdiction and culture-specific documents (National IT Security guidance documents)
• BS 7799
• Canadian Handbook on Information Technology (MG-9)
• The NIST Handbook
• MyMIS
Level 6
Domain and application specific documents, Industry guides
• German IT Baseline Protection Manual
• IETF RFC 2196 Site Security Handbook
• ISO/TR 13569 Banking and Related Financial Services-Information Security Guidelines
• CEN/ENV 12924 Medical Informations & Security Categorisation and Protection for Healthcare systems
• ISO/IEC 15947 IT Intrusion Detection Framework
World/Global
Nation/Organization
Site/Domain

Figure 1.1: Various Levels of Details of Standards and Documents

Level 5 of the model

Level 5 represents the three standards referred, i.e. BS 7799, the Canadian Handbook of Information Technology and the NIST. Documents under this group are categorised as jurisdictional and culture-specific. The MyMIS handbook is represented at this level.

Level 6 of the model

The standards within Level 6 are domain and application specific. Examples of such standards are the German IT Baseline Protection document, the IETF RFC 2196 Site Security Handbook, the ISO/TR 13569 on Banking and Related Financial Services, the CEN ENV 12924 on Medical Informatics: Security Categorisation and Protection Healthcare Systems and the ISO/IEC 15947 on IT Intrusion Detection Framework.

1.3 Handbook Coverage

This handbook describes safeguards, operational and technical issues and legal implications

This handbook provides the necessary guidelines on ICT security management safeguards to enable implementation of minimal security measures. It discusses elements of management safeguard, common operational and technical issues, and legal implications. The appendices at the end of the handbook may be of use to users with templates on security policies, adherence compliance plan, strategic plan, incident reporting mechanism, checklists and procedures. Its capacity is advisory and where the information contained is superceded (changes in technology, processes, legal requirements, public expectation) the reader is advised to refer to current adopted best practices.

ICT security management safeguards

The ICT security management safeguard identify five (5) major elements that should be considered by all public sector ministries, departments and agencies to protect their ICT systems. These elements are the ICT security policy, ICT security management programme, ICT security risk management, planning and incorporation of ICT security into the ICT systems life cycle and establishing ICT security assurance.

The handbook further explains some fundamental operational components of ICT security that is best recognised by public sector employees.

Technical details of ICT security

Technical security involves the use of safeguards incorporated into computer and communications hardware and software, operations systems or applications software and other related devices. This chapter explains the technical level of ICT security in greater detail.

Legal implications

The last chapter of this handbook briefly explains legal matters with respect to Malaysian law. It highlights Malaysian cyber laws and the various aspects of criminal investigations.

The appendices of this handbook provide some samples of framework, plan, checklist and forms useful in the ICT security management process.

1.4 Audience

Main objective is to provide guidance to all government employees

The main objective of this handbook is to provide guidance to employees within government agencies on the essential components of ICT security. It is intended to be the primary reference book used by all government employees in safeguarding the government's ICT assets.

The handbook is for ALL government employees

Various categories of government employees will benefit from the handbook as it covers a wide range of topics. Nevertheless this handbook is also useful to anyone wishing to learn about the application of ICT security.

Organisation of the content of the handbook

The handbook is presented in five (5) chapters that can be divided into three (3) different levels; Essential, Intermediate and Advanced (Figure 1.2). The Essential level, which comprises of Chapter 1, Chapter 2 and Chapter 5, provides fundamental knowledge on ICT security and is suitable for chief executives and managers in the public sector.

The Intermediate i.e. Chapter 3 is intended for general ICT users of the public sector. The description and explanation will provide guidance to users on the basic operational security safeguard to be implemented and maintained by them.

The Advanced stage i.e. Chapter 4 is proposed for the more experienced ICT administrators and managers. The descriptions on technical details of ICT security should provide guidance and direction on steps that need to be taken to ensure the confidentiality, integrity and availability of public sector ICT systems.

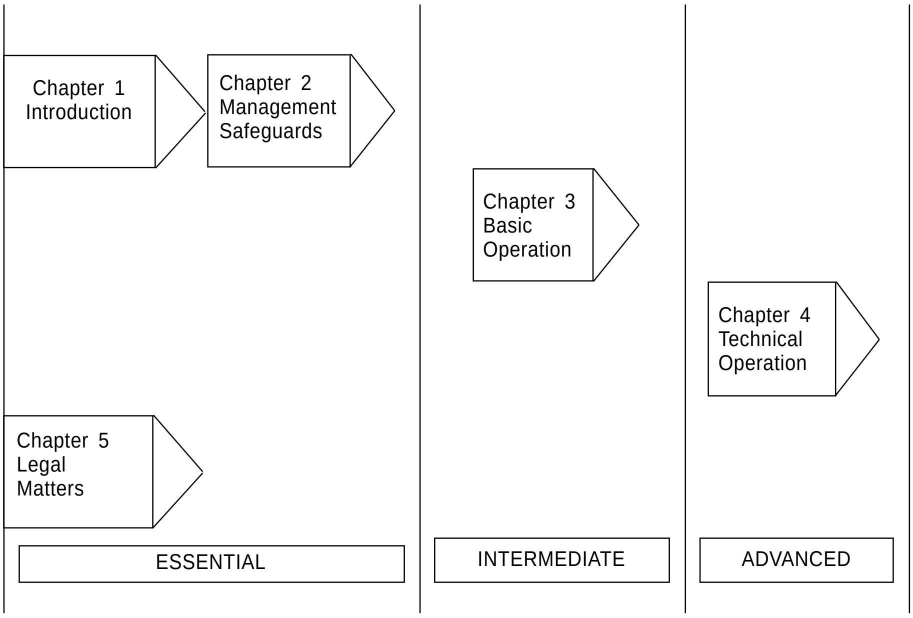


Figure 1.2: Malaysian Public Sector Management of ICT Security Handbook (MyMIS) Roadmap

Chapter 2 MANAGEMENT SAFEGUARDS

Senior management commitment

The main objective of this chapter is to highlight the major elements that should be considered by all government ministries, federal departments, statutory bodies, state secretaries and local authorities in their efforts to safeguard their respective ICT systems. Of utmost importance is senior management commitment towards acknowledging and addressing security issues.

5 major elements

The five (5) major elements of management safeguards are:

(a) Public Sector ICT Security Policy;

(b) Public Sector ICT Security Programme Management;

(c) Public Sector ICT Security Risk Management;

(d) Incorporating Public Sector ICT Security into ICT System's Life Cycle; and

(e) Public Sector ICT Security Assurance.

2.1 Public Sector ICT Security Policy

ICT Security Policy must ensure the government's information is secured

The government acknowledges its obligation to ensure appropriate security for all ICT assets under its ownership. This is best implemented by having a written ICT Security Policy that serve to assist in identifying at the very outset what needs to be protected. The document will also inform department members what activities are allowed or what activities are disallowed. The policy should define common rules to be abided by everyone within the organisation. The policy so formulated should address the need for a total enforcement of controls and measures to safeguard government ICT assets.

Policy needs to be balanced between rigid and loose information control

The tremendous increase in ICT dependency and usage especially with the advent of the Internet, exposes government information to a much larger audience and with that a potential threat that government information being compromised. This is especially worrying on classified government information and if left unchecked, can cause serious integrity issues to the government. At the same time, there need to be a balance between rigid information control that limits service delivery on one hand against a loose information control that would compromise security or severely affect the interest of the public service or the nation.

It is in realising the absolute importance of the provision of ICT security, the ICT Security Policy be drafted based on concrete ICT principles, best practices, responsibilities towards securing information, threats and incremental steps towards upgrading information security.

Important factors to consider in formulating the ICT Security Policy

Essentially the ICT Security Policy document should state:

(a) the ICT Security Policy statement;

(b) the rationale behind ICT security in protection against unauthorised access, ensuring availability and minimising security breaches;

(c) the ICT security definition inclusive of coverage of assets to be protected;

(d) the objectives of ensuring government operations continuity and to minimise disruptions by minimising impact of security incidents;

(e) the security principles adopted;

(f) the establishment of a clear management framework defining general and specific responsibilities for ICT security management, including reporting security incidents;

(g) the need for ICT security awareness training for all staff and specific security training for those with greater responsibilities; and

(h) the understanding of the requirement for shared responsibility in protecting government information.

There are three (3) different levels of Public Sector ICT Security Policy formulation. The higher level is the **Central Level** that provides the general policy direction. The next level is the **Ministry/State Level** that addresses specific issues and the **Departmental Level** handle operational issues.

2.1.1 Central Level

MAMPU is at the Central Level of formulating ICT policies for the public sector

This is the top most management level that initiates ICT Security within the public service. This role has been entrusted to Malaysian Administrative Modernisation and Management Planning Unit (MAMPU), Prime Minister's Department. MAMPU initiates and maintains the Public Sector ICT Security Policy Framework and is the referral centre on Public Sector ICT Security issues.

The high level policy issued as a General Circular 3/2000 dated 1 October 2000 *(Pekeliling Am Bil. 3 Tahun 2000 bertarikh 1 Oktober 2000)* provide the direction towards securing government ICT assets (Appendix A). The policy:

(a) defines the purpose and scope;

(b) assigns the responsibilities for programme implementation; and

(c) principles adopted.

2.1.2 Ministry/State Level

Specific issues affecting particular organisation

Issues addressed at this level are normally specific issues of concern affecting particular organisation or across the public service such as the disposal of unwanted computing equipment or backup of sensitive data.

Issue-specific level focuses on local areas or current issues

While the Central Level policy is intended to address the broad Public Sector ICT Security programme, the ministry/state level ICT management statements are developed to focus on specific areas currently relevant and of concern to the ministry/state.

Issue a plan of action

The management may find it appropriate, for example, to issue a plan of action on how the ministry/state should approach contingency planning (example centralised vs. decentralised) or the use of a particular methodology for mitigating a particular risk to ICT systems. Ministry/State wide plans may be appropriate when new issues arise, such as integration to legacy systems that may possibly require additional protection of some particular information.

While the Central Level broad-based policy may not require much modification over time, ministry/state policy formulation will likely require more frequent revision as changes in technology, demands, requirements, legislation and business rules take place.

2.1.3 Departmental Level

Operating at the action level

Operating or System-specific level focuses on actions taken to protect a particular system. This is operating at the action level where detail knowledge on procedures, standard, and guidelines are the daily norm.

The operating level or system specific provides detail information to address issues

While the Central and Ministry/State Specific Levels address issues from a broad perspective encompassing the entire organisation, they do not provide detailed information for example, on establishing application priorities, access controls and other specific requirements. This is where the departmental level or specific programme is needed.

The operating level security policy has important impact on system and its security

Departmental Level security policy is applied at the computer system operations level and may vary from system to system even within the same organisation. The departmental security policy has an important impact on system usage and safeguarding Public Sector ICT Security. The decision to adopt a departmental ICT Security Policy for the organisation can be made at the managerial level. Refer to Appendix D: Example of Contents List for an Agency/Department ICT Security Policy for guidelines on formulating policy.

2.2 Public Sector ICT Security Programme Management

Programme management is important

This sub-section discusses the importance of programme management and presents an organisation-wide approach in managing Public Sector ICT Security. Programme management among others encompasses nominating ICT Security Officers, developing security policies, carrying out security audits and providing ICT security incident response and handling services. In this respect, it is noted that the various ministries, departments and agencies in the public sector differ vastly in function, size, complexity, management style and culture.

2 different levels of programme management

In comparison to Public Sector ICT Security Policy formulation, there are only two (2) different levels of programme management. The higher level is the Central Level, which is responsible for overall strategy, co-ordination, planning and implementation as well as advice and direction on ICT security issues. Next is the Operating Level, which encompasses both ministry/state and department. ICT security programme management at this level details the procedures for implementing cost-effective ICT security.

2.2.1 Central Public Sector ICT Security Programme Management

Central Level ICT Security programme components

At the Central Level, ICT security programme management consists of the following:

(a) formulating Public Sector ICT Security Policy Framework;

(b) ICT Security Awareness and Training;

(c) ICT Security Incident Response and Handling;

(d) ICT Security Posture Assessment;

(e) ICT Security Business Resumption Plan Framework; and

(f) enforcement, audit and supervision.

Benefits of ICT Security programme

A central Public Sector ICT Security programme should provide three distinct types of benefits:

(a) Increased Efficiency and Economies of Scale of Public Sector ICT Security;

(b) Efficient, Economic Co-ordination of Information

A co-ordinated centralised programme can assist in the collection and dissemination of ICT Security related information efficiently throughout the Public Sector. Since it is centrally controlled, various information can be channelled directly to the respective Public Sector ICT Security Officer at the various agencies; and

(c) Central Enforcement and Supervision

One of the functions of the Central Level is the evaluation of enforcement activities and compliance. In this regard, the organisation needs to understand the business requirements, issues, vulnerabilities and Public Sector ICT Security discrepancies internally. This could be done through an internal supervisory function that allows a first-hand look at ICT issues without the potential embarrassment of an external audit or investigation.

2.2.2 Operating Level Public Sector ICT Security Programme Management

Scope of Operating Level Public Sector ICT Security Programme

Unlike the central programme that addresses the entire spectrum of Public Sector ICT Security, the operating level addresses the procedures for implementation of appropriate and cost-effective ICT security. Some of the salient items in considering the operating programme are:

(a) implementing safety measures;

(b) selection and installing of safety measures;

(c) day-to-day Public Sector ICT Security administration;

(d) evaluation of ICT system vulnerabilities; and

(e) responding to Public Sector ICT Security problems.

Local advocate

The local advocate for the security programme at this level is the ICT Security Officer (ICTSO). This officer is nominated by the ministry or department as suggested in the Public Sector ICT Security Policy Framework.

Copyright MAMPU

Action by ministry and department

At the operating level, the ministry or department should embark on:

(a) formulating departmental ICT security policy;

(b) undertaking ICT system life cycle management with respect to security;

(c) providing ICT security awareness and training;

(d) testing Business Resumption Plan; and

(e) conducting scheduled ICT security review.

2.3 Public Sector ICT Security Risk Management

Public Sector ICT Security is a continuous process

Need to ensure security is within an acceptable risk level

Security can be defined as a condition that is free from threats and unacceptable risks. Public Sector ICT Security should be looked upon as a continuous process. It involves periodic activities that must be implemented to ensure that security is within an acceptable risk level, taking into consideration technology change that brings with it rapidly changing threats and vulnerabilities.

Principal objective is to ensure business continuity

The principal objectives of securing ICT assets are to ensure government operations continuity and minimise disruptions or damage by preventing and minimising the impact of security incidents. ICT security aims at facilitating information sharing and simultaneously ensuring the protection of the information and ICT assets. In order to achieve the desired Public Sector ICT Security acceptance level, the vehicle used in assessing risk is aptly termed Public Sector ICT Security Risk Management. By definition, risk management is the process of assessing risks, taking steps to mitigate the risks to an acceptable level, accepting and monitoring the residual level of risks. A sample of ICT Security Risk Management process is as in Appendix E.

Steps for better risk management include identifying risks, evaluating risks and implementing safeguards

Steps required for better risk management includes:

(a) formation of a risk management committee;

(b) identifying the risks and threats;

(c) evaluating the risks and threats;

(d) identifying the necessary safeguards and counter measures;

(e) managing residual risk;

(f) implementing safeguard and monitoring effectiveness; and

(g) undertaking uncertainty analysis.

2.3.1 Formation of Risk Management Committee

Representation on Risk Management Committee

Risk analysis should be co-ordinated by the ICTSO and are best performed by a team of individuals representing the following disciplines:

(a) data processing operations management;

(b) systems programming (operating systems);

(c) systems analysis;

(d) applications programming;

(e) data base administration;

(f) auditing;

(g) physical security;

(h) communication networks;

(i) legal issues;

(j) functional owners; and

(k) system users.

2.3.2 Identification of Risks and Threats

Identifying risks and taking action

The identification of risks and threats is a critical step towards securing ICT assets. The result of the identification will dictate further activities and the channelling of resources, which consists of funding, training efforts and future planning. Hence, the proper planning of this activity cannot be overemphasised and should focus on avoiding core business shutdown or, at the least, minimising disruptions.

Unauthorised disclosure will cause embarrassment

In the public sector, unauthorised disclosure may result in embarrassment where the risk may not be quantifiable in terms of monetary loss.

In identifying the risks and threats, the ICTSO in consultation with the Chief Information Officer (CIO) and administrators will need to:

CIOs and the ICTSO need to discuss the risks and threats

(a) review the value of the information contained in their systems or information that could be derived from their information systems. Once this is done, the value attached to the ICT assets can help determine the level and types of risks that can or should be tolerated;

(b) determine events or combinations of events that could disrupt business operations. Admittedly, this is rather difficult to implement since the list could be endless. However most risks are visible and can be easily listed. Examples are physical sites, access controls, power supplies, environmental controls, etc.; and

(c) establish the priority to the risk elements identified. Some risks can have low priority whilst others are categorised as high priority risks. There is no rule to establish this, as risks are interpreted differently by agencies according to differing perceptions about the level of disruption or damage. In this light, the management may want to attach an association between risks, its potential disruptive ability and the cost of reconstruction.

The methods employed for identification of risks and threats may be formal (user observation reports), informal (corridor talk), quantitative or qualitative or a combination of these methods.

2.3.3 Evaluation of Risks and Threats

Evaluating risk through analysis of data and information

Once identification of risks and threats is completed, the process evolves towards risk evaluation, which involves the collection and analysis of data. There are many sources of information that can be used to conduct this exercise. Since information sources can be numerous, steps should be taken to screen and analyse the data. This can be performed by focusing on areas that have the greatest impact on the organisation. The following steps can be adopted in evaluating the risk:

(a) quantify the monetary value of a loss by considering these key elements in risk analysis:

i. an estimate of the impact or cost of a specific difficulty if it happens; and

ii. an estimation of the probability of encountering that difficulty within a period of time;

(b) determine the potential economic impact of those risks or events associated with each threat by using the list of vulnerabilities associated with the department's information assets identified in the previous step;

(c) estimate the probability of the undesirable events occurring within a specified period of time (usually one year). Identifying risks and their economic impact does not directly lead to identifying which security exposures are worth corrective action and which are not. Estimating and considering the likelihood or probability of the undesirable events is vital. For example, events such as floods or earthquakes have catastrophic consequences. However, if they appear to have a low probability of occurrence they might not justify protective measures and the decision may be to tolerate the risks;

(d) evaluate the suitability of the following options once the monetary value exposure or its annual loss is estimated:

i. tolerate the risk;

ii. insure against the risk;

iii. lower the monetary impact by implementing those measures costing less than the exposure; or

iv. lower the probability of the loss occurring by implementing protective measures costing less than the exposure;

(e) determine whether security safeguards are needed and if so, allocate the cost. The information gained from this can be used to estimate the annual monetary value of a loss, which subsequently can be used to provide a common denominator for determining the magnitude of each risk. A department may then develop safeguards against the high monetary loss risks; and

(f) identify alternative security safeguards and provide recommendations for cost-effective security solutions.

2.3.4 Identification of Necessary Safeguards

Identify the safeguards–could be additional or removal of ineffective safety measures

Amongst the key elements of Public Sector ICT Security is to identify suitable safeguards. The process of identification could result in acquiring additional safeguards or the removal of ineffective safety measures because both monetary and non-monetary factors are involved. For example, it may be effective from an economic and safety viewpoint to impose a new locking mechanism rather than to employ a security guard.

In the assessment of risks other than monetary issues, there will be areas where it is not obvious as to what kind of safeguard is appropriate.

ICTSOs and ICT managers need to consider many factors in identifying the safeguards

The other factors that should be considered by ICTSOs and ICT Managers are:

(a) legislation, regulation and organisation policy;

(b) user and business requirements;

(c) ICT system performance requirements;

(d) timeliness, accuracy, and completeness requirements;

(e) the life cycle costs of Public Sector ICT Security measures;

(f) the relative strength of the proposed safeguard;

(g) the reliance of other safeguards being considered;

(h) technical requirements; and

(i) cultural constraints.

2.3.5 Managing Residual Risks

Not possible to mitigate all risks and threats

Need to make decision on which ones

It is not possible to mitigate all risks and threats identified because, in reality, all ICT installations operate on limited resources. The management needs to decide what risks should and can be mitigated. The remainder of the risks not mitigated is generally known as residual risks. Once this type of risk has been identified based on priority ranking, a decision has to be made as to whether these risks are acceptable or otherwise. Managing residual risk should not severely affect the delivery of services and should be properly documented and monitored over time. Such residual risks should be quantified as far as possible and additional safeguards should be implemented if they are considered too high. The decision to balance between acceptable and unacceptable risk is a management decision.

2.3.6 Implementing Safeguards and Monitoring Effectiveness

Once decision is made-need for follow-through

Need to maintain, ensure it is ongoing

Need for periodic assessments

Once a decision has been made to implement the appropriate safeguards, the decision must be followed through. There is also the requirement that the safeguards be maintained and this process must be seen as ongoing, for inappropriate maintenance can render the safeguards ineffective. Also, it calls for periodic assessments to improve the safeguards with possible requirement for re-analysis of risk.

2.3.7 Uncertainty Analysis

Uncertainty analysis attempts to document grey areas

There will be instances when the management of risk relies on hearsay, speculation, best guess, assumption and incomplete data. Uncertainty analysis attempts to document this grey area so as to keep management informed and aware.

Two primary sources of uncertainty in the risk management process are:

(a) unknown precision of the methodology used; and

(b) difficulty to determine the exact value of the various elements in the risk model such as threats frequency, potential damage etc.

Projections and assumptions can be indeterminate.

It is possible that a data source is uncertain. Normally, data is collected from two sources; statistical data and expert analysis. However, there are potential problems from both sources. For example: samples taken may not be reflective of the true situation; missing or not properly counted parameters; misleading results and insufficient data. When expert analysis is done, it should be recognised that projections are subjective and the assumptions are always questionable.

2.4 Incorporating Public Sector ICT Security into the System Life Cycle

The purpose of incorporating the Public Sector ICT Security Plan into the ICT System Life Cycle is to ensure that the Public Sector ICT Security component is not overlooked. Since ICT has played an irreversible role in service delivery in the public sector, the planning of ICT systems should always include Public Sector ICT Security at the very onset. The Public Sector ICT Security Plan should be viewed as a documentation of the structured process to plan for adequate, cost-effective Public Sector ICT Security protection for the overall system.

2.4.1 Benefits of Integrating Public Sector ICT Security in the System Life Cycle

Might be too expensive to incorporate later.

Also can cause delay, disruption, etc.

It is recommended that the Public Sector ICT Security Plan be developed at the beginning and incorporated into the system life cycle. It would be difficult and expensive to redesign the applications to cater for security features at a later stage. Moreover, it can cause project delays, disruptions, diminish expectations and overall low morale.

Furthermore, it is virtually impossible to anticipate the whole array of security problems that would deter the incorporation of the Public Sector ICT Security Plan at the later stages of the system life cycle. Updating the security plan, at least, at the end of each phase in the system life cycle can minimise issues.

The documentation of decisions related to Public Sector ICT Security into the system life cycle should help assure management that Public Sector ICT Security is fully addressed in all phases including applicable legislation and other requirements.

2.4.2 The ICT System Life Cycle Phases

5 stages of ICT system life cycle.

It is recommended that planning for Public Sector ICT Security follow the stages described in most models of ICT System Life Cycle consisting of the following five (5) basic stages, incorporating ICT security issues in each stage and as depicted in Figure 2.1:

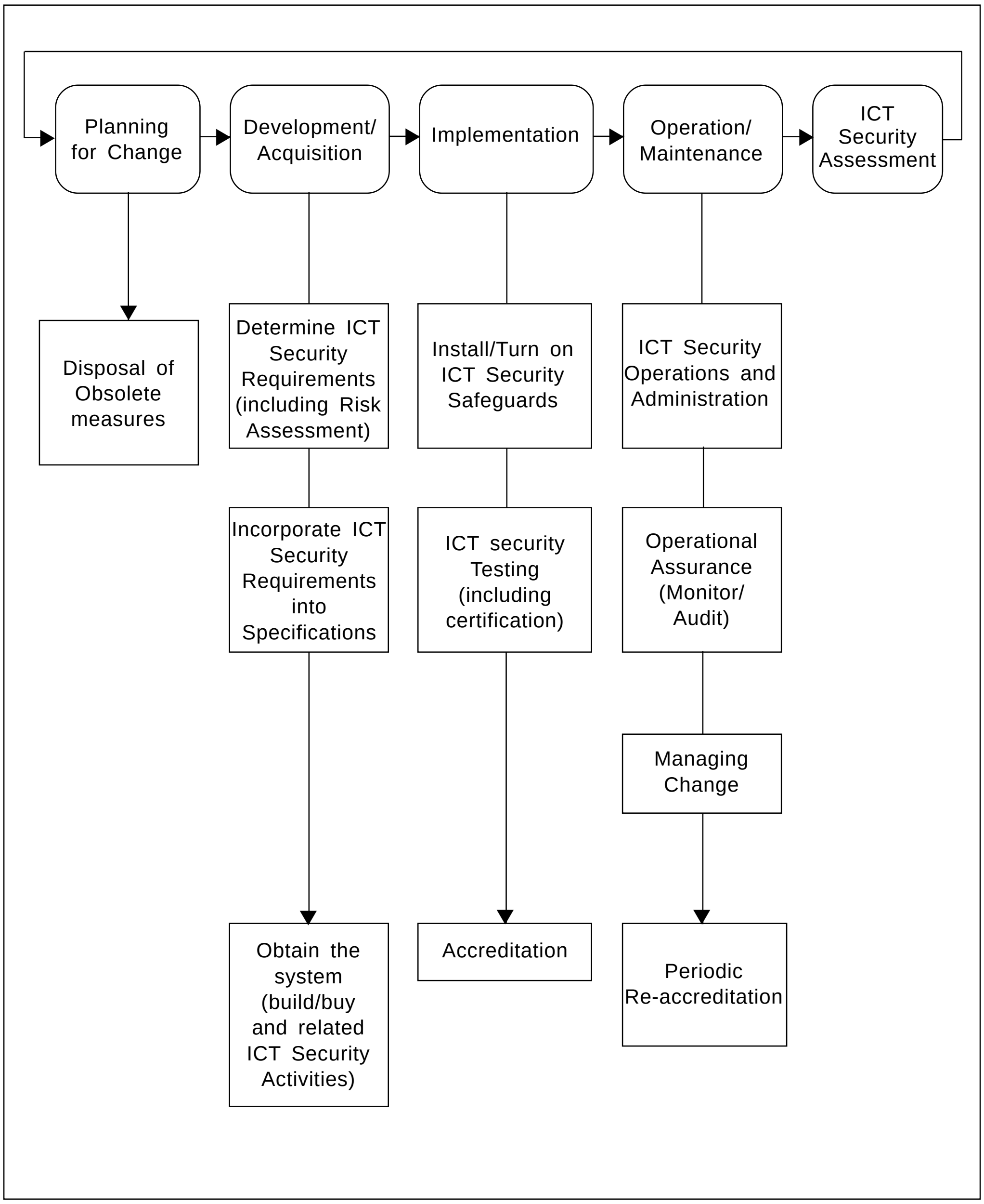

Planning for Change
Development/ Acquisition
Implementation
Operation/ Maintenance
ICT Security Assessment
Disposal of Obsolete measures
Determine ICT Security Requirements (including Risk Assessment)
Install/Turn on ICT Security Safeguards
ICT Security Operations and Administration
Incorporate ICT Security Requirements into Specifications
ICT security Testing (including certification)
Operational Assurance (Monitor/ Audit)
Managing Change
Obtain the system (build/buy and related ICT Security Activities)
Accreditation
Periodic Re-accreditation

Figure 2.1: ICT Security in the System Life Cycle Phases

1st stage: Planning For Change - This is to plan for the changes that will occur with the implementation of the new ICT system to meet operational and Public Sector ICT security requirements. This exercise can be very daunting, as it will involve practically everyone in the organisation especially in areas such as re-training, adaptation and the inception of completely new procedures.

2nd stage: Development/Acquisition - This is the stage where the ICT system is being constructed, programmed, developed or purchased. The Public Sector ICT security requirements based on core business functions, ICT asset value and risk assessment should be included in this stage.

3rd stage: Implementation - This is the stage where, upon final acceptance by the government, the ICT security safeguards are initiated.

4th stage: Operation/Maintenance - This is the stage where the developed system runs alongside the daily operations of the department. As the system matures, expansion through additional equipment and application systems is inevitable. New requirements may become apparent and obsolete functions may need to be removed.

5th stage: ICT Security Assessment - This is the stage where an assessment is made to determine whether ICT Security requirements are met.

At each of the five (5) stages, additions or deletions to the existing system may take place. Therefore the security aspects must be considered for each activity in every stage.

2.5 Public Sector ICT Security Assurance

2 rule of thumb questions.

The Public Sector ICT Security assurance means the confidence level in the Public Sector ICT Security safeguards to operate correctly as planned. The effectiveness of ICT security is not easy to assure because of the difficulty in quantifying assurance. As a rule of thumb, two (2) questions should be asked:

(a) who needs to be assured; and

(b) what type of assurance is required.

There are many methods and tools available. Two (2) of these are described below: Design and Implementation Assurance; and Operational Assurance.

2.5.1 Design and Implementation Assurance

The design and implementation assurance means that the design features of the ICT system, its operations or ICT assets must meet requirements and specifications. Assurances of this nature require the examination of the ICT system design, the correct functioning of each application and the manual processes that support it. Design and implementation assurance is associated with the development, testing, as well as pre- and post-implementation stages of the ICT system life cycle. The design and implementation assurance seeks to address whether the end product complies with the agreed Public Sector ICT Security specifications. It is also used to provide evidence of deviation and remedial action.

The following sub-sections suggest some of the major methods that can be adhered to in achieving design and implementation assurance.

2.5.1.1 Testing and Certification

Testing to ensure compliance to requirement and quality.

Testing is an activity to quantify compliance to stated requirements. In addition, it can be used to address the quality of the ICT system as it is being built, implemented and operated. Therefore, the testing should be performed throughout the development cycle or wherever proof of compliance is required.

Some examples of testing are;

(a) unit test;

(b) components test;

(c) system test;

(d) integration test;

(e) stress test; and

(f) penetration test (to see whether the safeguards can be bypassed).

Certification is formal testing conducted by an independent party. The appointment of such experts must conform to the current government procedures pertaining to the appointment of consultants. *(Refer to Surat Pekeliling Perbendaharaan Bil. 3 Tahun 1995 – Peraturan Perolehan Perkhidmatan Perunding).*

2.5.1.2 Conformance Testing

The organisation may conduct conformance tests on products such as software, hardware and firmware. Conformance to ICT standards is important to ensure the inter-operability or strength of ICT security.

2.5.1.3 Use of Reliable Architectures

Need to use reliable architecture.

The use of reliable architecture such as fault-tolerance, redundancy and mirroring enhances the degree of assurance of ICT systems. However the use of costly reliable architecture is normally reserved for very critical systems that demand practically zero fault.

2.5.1.4 Ease of Safe Use

Ease of safe use of Public Sector ICT Security products and mechanisms is another important aspect of the successful implementation of Public Sector ICT Security systems. When the interface with safeguards is easy and straight forward, the tendency is that the user is more likely to use the system correctly and commit fewer mistakes. Thus, acceptance by the users enhances the overall security assurance.

2.5.1.5 Evaluation and Reviews

Product evaluation and review will help achieve assurance.

Evaluation and reviews are another option for achieving assurance. Product literature in reviews provides useful information and is normally geared to product superiority above other similar products. However, product reviews are less formal and do not offer detailed and extensive examination as is available through an evaluation.

Important factors to consider when attempting to seek comfort level via this means are as follows:

(a) independence of the review group;

(b) evaluation criteria;

(c) testing parameters;

(d) competence;

(e) integrity of the evaluating body; and

(f) assumptions made.

2.5.1.6 Assurance Documentation

Describing how ICT security requirements are met.

Assurance documentation is one that describes Public Sector ICT Security requirements and how they are met when compared against these requirements. The significance of assurance documentation is the indication of the degree of understanding as portrayed by the designers, and their presumed ability to construct solutions to meet the necessary Public Sector ICT Security requirements. Please refer to Appendix F: A Sample ICT Security Adherence Compliance Plan for guidance on compliance programmes.

2.5.1.7 Certification of Product to Operate in Similar Situation

Assurance to operate products in different environments.

There will be instances when a department seeks clarification that the ICT Security product it is about to procure operates seamlessly in its current environment. This may be the case for departments that operate on proprietary systems wishing to employ products outside their operating environment.

Most producers of ICT Security products, with very good reputation produce documentation, brochures and advertisement statements of certification of their ICT Security products that operate in similar situations. However, it should be realised that certification to operate in a similar situation is environment specific, since it may be certified to operate in one environment but may not work in another, even though the certification is performed by the same body.

The risks are high if the products to be procured and used at the required department are non-certified products. It might be a better decision to opt for other certified products. Certification should be nationally accepted.

2.5.1.8 Self-Certification

Test conducted by vendors or suppliers can be indicators.

In many instances the software vendor or the system integrator of the ICT Security system conducts self-certification of their own products. This is done to determine or at least provide some indication the quality and performance of their products. This technical evaluation may not be partial but does provide a minimum degree of assurance. In cases where a high degree of assurance is required, a third party independent evaluation is recommended.

2.5.1.9 Warranties and Liabilities

Undertaking to correct errors and provide upgrades.

This is another form of assurance where the manufacturer or integrator provides an undertaking to correct errors or provide upgrades via version releases. It can be in the form of a formal declaration or certification of the product or published assertion. The manufacturer’s commitment is seen through its endorsement to correct errors and indemnify loss or damage should the product be non-conforming.

Assurance by digital signature, anti-virus software.

2.5.1.10 Distribution Assurance

The assurance of ICT products obtained via electronic distribution is important. In such a situation, the distribution of unmodified copies and its integrity can be ascertained through the use of digital signature or check-bits. Sources downloaded from unknown origin such as bulletin board should be verified by anti-virus software at the very least.

2.5.2 Operational Assurance

Operational assurance addresses technical issues.

Whilst design and implementation assurance addresses the quality issues, operational assurance seeks to address technical features such as vulnerabilities, conformance to procedures and changes to Public Sector ICT Security requirements. The ICT system being a ‘living’ system changes over time. Some causes of change include changes to the ICT system due to expansion of scope, operating systems or threat environment.

The operational performance of ICT systems tends to degrade over time. Creative users and operators resort to new ways to bypass Public Sector ICT Security measures with the sometimes incorrect perception that it may improve performance. It is very rare where adherence to procedures is strictly followed. In some instances this can produce disastrous results for the administration of the ICT system.

There are two basic methods to observe operational assurance:

(a) ICT System Audit

This can be either a scheduled or an unscheduled event to evaluate Public Sector ICT Security. It is important to define the scope of work since the auditing process can easily be side-tracked towards less important issues. The auditing process can both be investigative in nature (to resolve specific issues) or developmental.

(b) Monitoring

This is one of the most effective mechanisms to ensure operational assurance. However this activity is time consuming and requires more resources. It involves periodic checks on the overall ICT system including user activities, standard operating procedures, the environment etc.

2.5.2.1 Audit Methods and Tools

Auditing needs to be developmental rather than fault-finding.

All audits conducted on public sector ICT installations, environments or premises should follow stated or implied Public Sector ICT Security Policy and Public Sector ICT Security Auditing Guidelines or other documents published later. In conducting the ICT audits, the audited department plays a crucial role in extending assistance. The audits have to be treated as developmental and not as a fault-finding exercise. It is best for the government if the audited department and the audit team identify the appropriate Public Sector ICT Security requirements (which may be additional) based on the existing ICT environment. The audit conducted should not interrupt the business operation of the audited department. Three (3) different types of auditing methods with respect to depth and objectives are described in the following paragraphs.

(a) Audit Methods

i. Public Sector ICT Security Review

Public Sector ICT Security Review can be conducted by internal staff. This review is comparative in nature and is regarded only as informative. Reviews are normally conducted for a short duration but its preliminary initial results may lead to more advanced and detailed types of audits.

ii. Internal Audit

The internal audit measures the compliance of the ICT systems. The results of this exercise could be used as a guide even though there may be a conflict of interest.

In every environment, the internal staff is more knowledgeable in the ICT system installation, system security, etc than a third party. Hence the internal audit review is a required step to be performed.

Inadequacy of an internal review is that a poorly designed or poorly operated security system could still be acceptable. On the other hand, there could be a strong desire to improve the Public Sector ICT Security system.

iii. External Audit

In comparison, external auditing involves a third party that has no stake in the ICT systems. The independent party should review the ICT system installation, system security, etc.

In all three cases it is important to ensure that auditing personnel possess sufficient knowledge of Public Sector ICT Security.

Suitable generic auditing tools for the various types of audit described above are briefly explained below:

(b) Audit Tools

i. Automated tools (active and passive tools)

Tools for auditing the Public Sector ICT Security system.

The use of automated tools reduces the amount of work that has to be completed. It is used to identify a variety of threats and vulnerabilities such as improper access control, weak password or failure in using current up-dates and patches.

Active automated tools are designed to locate vulnerabilities by trying to exploit them. Passive automated tools examine only the ICT system and infer the existence of problems.

The government’s Public Sector ICT Security could be in a difficult situation if automated tools are not used. This is primarily due to the fact that hackers use similar tools to identify weaknesses of the ICT system.

Some of the current automated tools are easier to use while others require specific skills and pre-requisites.

ii. Internal control audit

These tools are used to determine the effectiveness of control or safety measures. It includes analysis on both ICT and non-ICT based controls or safety measures. Techniques used include inquiry, observation and testing to detect illegal acts, misuse, errors, irregular incidents or a general lack of compliance

iii. Security checklist

This is a tool normally developed by system owners to ensure that changes to the ICT system configuration has been reviewed. The checklists should be formulated to reflect local operation of an ICT installation.

iv. Penetration testing

The penetration test could be used as a tool to emulate the real life situation of potential attackers attempting to break into ICT systems. Findings from the tests are used to overcome vulnerabilities and weaknesses. On conducting such tests the ‘attackers’ should be using tools as would be used by the genuine attacker such as:

* automated tools as described previously;

* manual penetration;

* internet tools; and

* social engineering.

2.5.2.2 Monitoring Methods and Tools

Public Sector ICT Security need to be monitored continuously.

The ICTSOs and senior management in the public sector need to be sensitive to the vulnerabilities of the Public Sector ICT Security and react to ICT incidents. Thus it is important that the monitoring of the entire Public Sector ICT Security should be treated as an on-going process.

Many tools are available today and there are more being developed to handle new and complex attacks on ICT establishments. Below are some of the tools used for monitoring which also complements tools used in auditing. These tools enable monitoring to review ICT systems regularly and in real time. Access to audit tools, tabulation analysis and recommendations should be restricted and authorised.

(a) ICT System Logs

A documented evidence and a chronological event of all ICT system activities. This log should consist of information such as identification of unauthorised access, unexplained or abnormal activities. The logs should be viewed regularly in order to verify the usual and/or unusual activities in the ICT system.

Best practice : View and check the log daily on critical or sensitive systems.

(b) Automated tools

i. Virus Scanners

Readily available on the market both for stand-alone or networked systems. All users should use anti-virus software to verify the integrity of their systems. However, it should be noted that the threat from virus requires periodic up-dates of the anti-virus software

Best practice: Up-date anti-virus software regularly.

ii. Check Summing Algorithm

Work by generating mathematical value based on the contents of the file. Verification of the file is done by comparing the value of the sum generated by the current file with the previously generated value. The integrity of the file is verified when the two values are identical. Another common tool is the digital signature, which is also used to verify the integrity of the files.

Best practice: Ensure the check summing tools are run on the new installation, clean version and check sum value are stored securely.

iii. Password Crackers

These are specialised software to check against proper user passwords as compared to easily guessed passwords.

Best practice: Run monthly.

iv. Integrity Verification Programmes

Some of the techniques applied in integrity verification include consistency check, sensible checks and validation during data entry and processing. The objective is to ensure that the data is not tampered, omitted or unintentionally entered by way of examining data elements and expected relationships.

Best practice: Incorporate during planning, design and programming stage.

v. Intrusion Detectors

These are online applications used to analyse log-in activities, connections, operating system calls and other various command parameters to detect intruders.

Best practice: Use for critical system.

vi. ICT System Performance Monitoring Analysis.

This programme analyses system performance in real time to look for items such as abnormal system response time or abnormal request for resources.

Best practice: Run constantly at the background. Consider adequate lead-time for remedial action.

Improving operational assurance addresses technical issues.

2.6 Operational Assurance Issues

Several issues are addressed and recommended to improve the operational assurance.

(a) Encouragement in the Usage of Locally Developed Security Products

Locally developed security products are preferred over foreign makes to help spur local ICT security development.

(b) Network Auditing

Network auditing methods and tools should be use to ensure the security of the network and to simplify the management of network auditing. Examples of automated auditing methods are the checking and verifying of the data packet from one terminal to the other.

(c) Analysis of the ICT System Activity Log

The ICT system produces the ICT system log. This could be a daily, weekly, monthly or other time-based activity log. It is a detailed log that indicates the user’s activity. The log should be checked and reviewed by the ICTSO or by internal or external auditors.

(d) Maintenance Contract

Maintenance clauses should be incorporated into Sales and Purchase Agreement to include provisions for hardware maintenance by the supplier during the warranty period. In some cases it may be necessary to stipulate the service level required.

(e) Standard Operating Procedures

Standard Operating Procedures should be documented and formalised.

Chapter 3 BASIC OPERATIONS

This chapter discusses fundamental operational components

To implement effective Public Sector ICT Security will require strong commitment from the various level of organisations within the government. ICT security as a programme encompasses a wide spectrum of topics such as technology, people, finance, training, policy, risk management, processes and measures taken in total to safeguard the government's information and communications systems. This chapter explains some fundamental operational components of ICT security that should be imparted to public sector employees. Major areas include information classification, roles and responsibilities, human factors, electronic facilities, document management, storage management, contingencies, incident handling and physical and environmental protection.

3.1 Information Classification

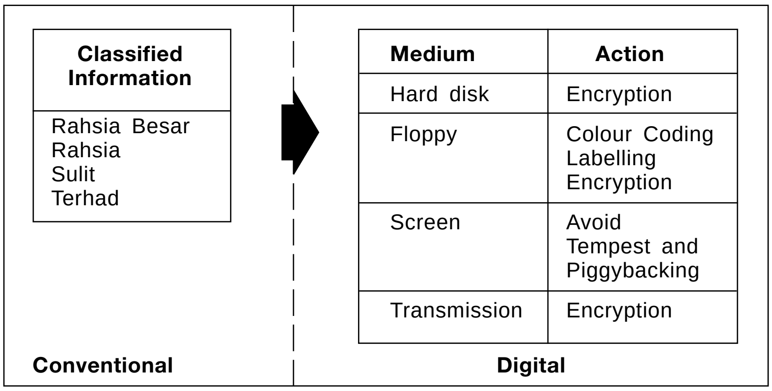
4 classifications of official matters–Rahsia Besar, Rahsia, Sulit and Terhad

Official matters are graded into four classifications i.e. *Rahsia Besar, Rahsia, Sulit* and *Terhad* as stipulated in the *Arahan Keselamatan.*

Information content created digitally follow similar classification. However the protection of digital information requires different handling needs when compared to paper-based information such as encryption, colour coding, labelling, precaution against piggybacking and electronic eavesdropping e.g. tempest (Refer to Table 3.1 and Figure 3.1).

Mode	Conventional	Digital
Media	Hard copy	Digital Information
Handling	As per *Arahan Keselamatan*	Handling protection (As per Figure 3.1)

Table 3.1: Conventional vs. Digital Information Handling



Classified Information
Rahsia Besar Rahsia Sulit Terhad

Medium	Action
Hard disk	Encryption
Floppy	Colour Coding Labelling Encryption
Screen	Avoid Tempest and Piggybacking
Transmission	Encryption

Figure 3.1: Handling Protection

3.2 Roles and Responsibilities

Management involvement is critical to ICT security. Capital expenditures alone cannot accomplish security. Management concern and effort are needed to plan, guide, motivate, and control an effective ICT security programme via the formation of ICT Security forum. A balanced programme, with proper concern for practicality and human values, will enhance the overall effectiveness of the information processing function.

3.2.1 Head of Department

Roles of Head of Department

Heads of Department are owners of Public Sector ICT assets and are accountable for their safe-keeping and protection. Essentially, the Head of Department should realise the importance of Public Sector ICT Security before it is implemented across the entire organisation. The Head of Department needs to be responsible for and supportive of ICT security programmes, promote compliance to standards, procedures and guidelines, and align Public Sector ICT Security requirements to the department's missions and objectives. In addition, the Head of Department should ensure adequate resources, both financial and personnel, are available for the programmes.

The roles and responsibilities of the Head of Department include:

(a) ensure all users including government employees, vendors and contractors understand the need for Public Sector ICT Security policy, standards and guidelines;

(b) ensure all users including government employees, vendors and contractors abide by the Public Sector ICT Security policy, standards and guidelines (necessary action must be taken upon non-compliance of any security measure);

(c) undertake evaluation of risk and security programmes based on the Public Sector ICT Security policy, standards and guidelines;

(d) develop an Adherence Compliance Plan for the purpose of managing risk arising from non-compliance of the Public Sector ICT Security policy, standards and guidelines; and

(e) report to MAMPU and other relevant authorities as required under *Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) - Pekeliling Am Bil. 1/ 2001* dated 4 April 2001 the following:

i. information loss or unauthorised information disclosure or suspected information loss or suspected unauthorised disclosure;

ii. unauthorised or suspected unauthorised usage of ICT system;

iii. loss, stolen or unauthorised disclosure of access control mechanisms or passwords or suspected loss, stolen or unauthorised disclosure of access control mechanisms or passwords;

iv. unusual systems behaviour such as missing files, frequent crashes and misrouted messages; and

v. attempted ICT break-ins and untoward security incidents.

3.2.2 Chief Information Officer

Roles of CIO–Strategic Planner of Public Sector ICT Security

The Chief Information Officer (CIO) is another important ICT resource person. The roles and responsibilities of the CIO include:

(a) support the Head of Department in discharging Public Sector ICT Security responsibility;

(b) transform the responsibilities above into an effective action plan;

(c) incorporate Public Sector ICT Security requirements into existing CIO functions i.e. preparing the IT Strategic Plan. A sample ICT Strategic Plan is as per Appendix G; and

(d) in some cases, the CIO is also the Departmental Security Officer.

3.2.3 Computer Manager

Roles of Computer Manager

The Computer Manager acts as the Operational Head of ICT and is responsible for managing Public Sector ICT Security at site.

The Computer Manager supervises and monitors personnel in the department and acts as the key player in ICT security programme.

The roles and responsibilities of the Computer Manager include:

(a) understand, support, and abide by the Public Sector ICT Security Policy, standards (MS ISO/IEC 13335 part 1-3, MS ISO 17799 part 1) and MyMIS;

(b) ensure that all users understand, support and comply with the Public Sector ICT Security policy, standards and guidelines;

(c) implement ICT security controls consistent with the requirements of the department;

(d) create a positive atmosphere that encourages all users to report on ICT security concerns;

(e) define realistic ‘need-to-know’ or ‘need-to-restrict’ criteria to implement and maintain appropriate access control;

(f) review physical security safeguards, in consultation with the Chief Government Security Officer, Public Sector ICT Security officer and others, as required. (Physical security should not only address the central ICT installations only but also back-up facilities and office environments);

(g) ensure that ICT security reviews are performed as and when required either by internal policy, regulations or ICT security concerns. Some examples of circumstances that trigger such a review include:

i. large loss from a security failure;

ii. purchase or upgrade of computer systems or software;

iii. acquisition of new communications services;

iv. introduction of new tools;

v. introduction of new out-sourced processing vendor; and

vi. discovery of a new threat or a change in a threat’s direction, scope or intent.

(h) develop, review and align the contingency planning of the department;

(i) review the entry and exit procedures in terms of user accessibility to system resources when employees join or leave the department;

(j) apply security principles in preparing exception requests;

(k) ensure subordinates participate in the ICT security awareness programme;

(l) report any ICT security concerns to the CIO; and

(m) periodic review of access rights and privileges.

3.2.4 ICT Security Officer

The ICT Security Officer (ICTSO) is in charge of the development, implementation and maintenance of the Public Sector ICT Security programmes of the department.

Roles of ICTSO

The roles and responsibilities of the ICTSO include:

(a) manage the overall Public Sector ICT Security programme of the department;

(b) enforce the Public Sector ICT Security policy, standards and guidelines for use throughout the department (these documents should be kept up-to-date, reflect changes in technology, organisation's direction and potential threats);

(c) assist in the development of specific standards or guidelines that meet Public Sector ICT Security policy requirements for specific applications within the department;

(d) review ICT systems against stated security requirements to identify vulnerabilities and risks;

(e) perform Public Sector ICT Security audits based on accepted Public Sector ICT Security policy, standards and guidelines to identify non-compliance;

(f) ensure that when exceptions to policy are required, the risk acceptance process is adhered to and that the exception is reviewed and re-assessed periodically;

(g) suggest measures to bridge the gap in the case of non-compliance;

(h) review audit and examination reports dealing with ICT security issues and ensure that management understands the Public Sector ICT Security issues involved. The ICTSO should be involved in the formulation of management's response to the audit findings and follow-up periodically to ensure that controls and procedures required are implemented within the stipulated time frame;

(i) confirm that the key threats to information assets have been defined and understood by management;

(j) keep up-to-date on current threats, information processing technologies and the most current information protection methods and controls through periodic information up-dates, ICT security seminars and on-the-job training;

(k) prepare and disseminate appropriate warning of potentially serious and imminent threats to the organisation's information assets, e.g. computer virus outbreak;

(l) form a security handling team to handle security incidents;

(m) co-ordinate or assist in the investigation of threats or other attacks on information assets;

(n) assist in the recovery from attacks;

(o) assist in responding to department's client security issues, including letters of assurance and questions on security; and

(p) report any Public Sector ICT Security issues to Departmental Security Officer and CIO.

3.2.5 System Administrators

Roles of System Administrator

The roles and responsibilities of System Administrators include:

(a) maintain the accuracy and completeness of access control privileges based on instructions from the information resource owner and in accordance with applicable Public Sector ICT Security policy, standards and guidelines;

(b) take appropriate action when informed by the respective manager whenever employees terminate, transfer, take leave of absence, or when job responsibilities change;

(c) closely monitor users with high-level privileges and remove privileges immediately when no longer required;

(d) monitor daily access activity to determine unusual activity such as repeated invalid access attempts that may threaten the integrity, confidentiality or availability of the system (these unusual activities, whether intentional or accidental in origin must be brought to the attention of the ICTSO for investigation and resolution);

(e) ensure that every user be identified by a unique identification (user ID) associated only with that user (the process should require that the user identity be authenticated prior to gaining access to the information resource by utilising a properly chosen authentication method);

(f) make periodic reports on access activity to the appropriate information owner; and

(g) ensure that audit trail information is collected, analysed and protected.

The System Administrator's activities should be reviewed by the ICTSO or any authorised independent party on a routine basis.

3.2.6 Help Desk

Roles of Help Desk

The main function of the Help Desk is to provide quick assistance to users on problems and issues related to computer applications and set-up. The Help Desk is the first point of reporting on ICT incidents and to re-route callers to responsible personnel. A sample of Help Desk Reporting Form is attached as in Appendix I.

3.2.7 Users

Responsibilities of users

By definition, a user is anyone who accesses any government ICT asset. A user may be a government employee, members of the administration, contractors, vendors or anyone who accesses or uses government ICT assets.

All users are held responsible for their actions when accessing government ICT assets. This accountability should be made clear to all potential users. In order to ensure compliance, all ICT systems should support facilities that record and detect user actions.

The roles and responsibilities of users include:

(a) understand, support, acknowledge and abide by the Public Sector ICT Security policy, standards and guidelines;

(b) aware of the security implications of their actions;

(c) promptly report to relevant authorities any suspicious behaviour or circumstance that may threaten the integrity of information assets or processing resources; and

(d) keep each department's information confidential.

3.2.8 Vendors, Contractors and External Service Providers

Responsibilities of Vendors, Contractors and External Service Providers

The responsibilities of Vendors, Contractors and External Service Providers include:

(a) understand, support and abide by the Public Sector ICT Security policy, standards and guidelines;

(b) be aware of the security implications of their actions;

(c) promptly report to relevant authorities any suspicious behaviour or circumstance that may threaten the integrity of information assets or processing resources; and

(d) keep the government's information confidential.

3.3 Human Factors

Employees are important assets

For any department, the employees are its most important assets. Through proper planning of acculturation, employees can and do contribute successfully to achieving the mission and vision of the department.

Employees play crucial roles in supporting departmental security ICT programmes. Armed with proper training, most employees can be depended upon to identify anomalies and deviations from good security practices, which can then be the basis for remedial actions. It is also useful to note of cases where employees take advantage of vulnerabilities resulting in theft, information exposure or wrongful communication. Employees also commit mistakes whether intentional or otherwise that may later lead to security breaches.

Statistics also indicate that employees perpetrate computer crime in lieu of their intimate knowledge on internal systems.

Mobilising human resources

To mitigate the risks mentioned above, government department should consider developing suitable approaches in identifying vulnerabilities that could be taken advantaged off by employees. A good case in point is the ICT hierarchy where certain positions become sensitive due to its association with powerful privileges. In such case, all personnel earmarked to such positions should be thoroughly vetted. It is also good practice for management to “know their employees” so that such intangible factors such as attitudes and inclinations may be known. Some of the controls listed below represent safeguard in human factors.

3.3.1 Personnel Security

Reducing security risk from errors

Personnel security encompasses activities aimed at minimising security risk caused or originating from employees resulting from errors and or oversight.

Safeguards include:

3.3.1.1 Confidentiality Agreement

Confidentiality declarations and agreements

Employees that are privy to sensitive information will be required to sign a non-disclosure agreement. (A good example is as per *LAMPIRAN 'D' of Arahan Keselamatan*).

The original copy of the duly signed agreement should be retained for safekeeping and future reference.

3.3.1.2 Personnel Screening

Personnel screening should be addressed at the recruitment stage

Personnel screening calls for the vetting of government personnel and as practiced, implemented at the recruitment stage. There may also be instances where the employee is subjected to detail vetting due to scope enlargement or promotion.

All matters pertaining to personnel screening should be referred to the Office of the Chief Government Security Officer.

No automatic right of access

No automatic right of access will be granted to individuals regardless of their security vetting. In all instances of information exposure, the need-to-know principle must prevail.

3.3.2 Awareness

Head of Department should establish awareness programme

Employees should inculcate good ICT Security practices. This could be achieved by establishing an ICT communications and awareness programme to inform employees of the importance and seriousness of ICT security. In order to further minimise risk, a 'clear desk' policy should be implemented.

Clear desk can be defined as not leaving sensitive materials on desk when left unattended.

3.3.3 Problem Employees

Assist problem employees

Employees with personal problems that could result in possible ICT security exposures should be given assistance.

3.3.4 Former Employees

Surrender all properties

Employees who leave the organisation must surrender all organisational assets under the employee's supervision immediately.

3.4 Electronic Facilities

3.4.1 Telecommuting

Telecommuting and remote accesss

The current technology has enabled users to initiate work from anywhere and at the same time remain connected to the office. This facility or telecommuting allows mobility and users access into the office ICT system.

The following should be considered in addressing security issues for telecommuters:

(a) equipment borrowed must be with a prior approval from head of department. The employee is accountable for the safety of the borrowed equipment;

(b) allow an employee to telecommute only after consideration is given to the employee's interpersonal skills, communication skills, and ability to work in an unsupervised environment;

(c) establish and distribute a clear written procedure on telecommuting; and

(d) require any employee who wishes to telecommute to execute a written agreement which addresses the following issues:

i. equipment to be used;

ii. phone lines;

iii. maintenance;

iv. costs and reimbursements;

v. supervision;

vi. liability for personal injury, fire, etc.; and

vii. physical and logical security to include protection of equipment, information transmitted or stored, hardcopy, back-up of information, disposal of hardcopy and diskettes, and protection of networks.

3.4.2 Voice, Telephone and Related Equipment

Telephones, PBX, facsimile and Voice Mailboxes are the penetration points

Telephones, Private Branch Exchange (PBX), facsimile machines and Voice Mailbox systems are frequent penetration point and are also open to abuse. The most common security hole is the use of insecure maintenance modes/interfaces.

PBX attacks often result in attackers making long distance telephone calls, perhaps completely unnoticed until bills suddenly increase. Often maintenance modes are badly protected or special features are enabled for outside access when they should not be.

In general, they are subjected to the following:

(a) where possible, maintenance interfaces should not be accessible externally;

(b) maintenance passwords should never be left at their default settings; and

(c) all devices with external interfaces should be configured such that they are not easily open to abuse.

Voice mail systems are subject to threats and exposures

Organisations utilising voice mail systems are indeed subject to a variety of potential threats and exposures. This includes disclosures of messages, liability for long distance telephone charges and possible loss of service due to unauthorised access to voice mail systems. It is completely necessary to get the ICTSO involved in the implementation and review of appropriate security controls offered by vendors. This will eliminate or reduce possible security exposures.

The following subsections illustrate control mechanisms that should be used to secure voice and related information.

3.4.2.1 Access to Voice Mail System

Control access to voicemail service

The integrity of information residing in voicemail can be preserved and the expenses and liability of unauthorised use of voicemail services limited by controlling access to voicemail service with physical controls and with logical access controls.

3.4.2.2 Private Branch Exchange

Control access to PBX

A PBX is an internal switch for attached telephone units within an organisation. The switch usually supports connections to outside telephone lines and may support electronic switching of information to the attached computer devices.

PBX systems can be protected against unauthorised outside calls as well as unauthorised disclosure, modification or destruction of information via its electronic components by:

(a) maintaining close liaison with the PBX supplier and network service providers concerning emerging fraud and other problems;

(b) providing physical access controls that restrict access to the PBX by authorised individuals;

(c) protecting any maintenance or administrative ports that are accessible via remote dial-up, with passwords, and either require secure call-back or challenge/response procedures;

(d) producing an audit trail of all administrative and maintenance access;

(e) changing all default password settings immediately upon installation of a PBX;

(f) documenting all changes following approved change control procedures. It may be necessary to use call accounting software;

(g) preventing all access to local ‘hot numbers’ or other expensive services; and

(h) following least privilege on setting facilities for particular extensions, e.g. deny international access unless explicitly authorised.

3.4.2.3 Spoken Word

Control access to spoken word

It is completely necessary to educate employees to the sensitivity of information being discussed regardless of circumstances by advising employees periodically and to be aware of who is present during conversations involving official secret information. Whenever official secret information is to be discussed, an announcement to that effect should be made, unless it is clear that persons who are party to the conversation or meeting are aware of the sensitivity of the information.

3.4.2.4 Intercept

Interception during transmission

Communication can be intercepted. The prevailing technology has made the process simpler and can be mounted within a short time span. Therefore, it is advisable that organisations protect against interception of official secret information during telephone transmission by:

Encrypt communications to prevent interception

(a) encrypting telephone calls in which official secret information will be discussed; and

(b) prohibiting use of unencrypted cellular or cordless telephones for transmission of official secret information, except in emergencies.

3.4.2.5 Casual Viewing

Minimise casual viewing

In order to minimise the disclosure of information on computer terminal screens through casual viewing:

(a) position computer displays away from public view;

(b) implement password screen saver; and

(c) apply the need-to-know principle.

3.4.2.6 Output Distribution Schemes

Destroy unused hard copy

There is a trend to replace paper documents such as reports and statements with on-line access to computer systems.

In order to protect against unauthorised modification of official secret information reports, destroy unused hard copies completely.

3.4.2.7 Destruction

Dispose unused official secret information

All unused official secret information should be disposed of securely and completely.

3.4.2.8 Clock Synchronization

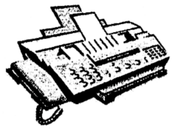
Set the computer clock correctly

It is important to ensure correct setting of computer clocks. This will become apparent when determining sequence of events and audit trail.

3.4.3 Facsimile

Control access to the facsimile

Facsimile is the transmission of paper-based text, graphs, drawings, plans and other written images electronically via telephone lines.



Since the fascimile allows for the transmission, receipt and hence the dissemination of information, suitable controls should be implemented to govern its use:

(a) all facsimile machines should be installed in rooms that are visible and be easily monitored;

(b) allow personnel with granted access privileges to pick up messages; and

(c) the transmission of official secret information when done through facsimile should only be done using secured facsimile machines approved by the government.

3.4.3.1 Modification

Employ separate verification

To preserve the authenticity of the source documents, employ separate verification means such as prearranged telephone calls to confirm transmission and receipt.

3.4.3.2 Transmission Acknowledgement

Use of transmission acknowledgement

In preventing false claims of message receipt or denial of message delivery, apply transmission acknowledgement controls such as transmission acknowledgement and telephone confirmation.

3.4.3.3 Misdirection of Messages

Check identity of the receiver

To avoid misdirection of official secret information and hence disclosure, re-check the receipient number and identifying prior to sending.

Attach appropriate warning coversheets to assist in the retrieval of facsimile documents at the receiving end and also to assist in detecting misdirected facsimile messages.

3.4.3.4 Disclosure

Encrypt facsimile for official secret transmission and prevent unauthorised viewing

All transmission of official secret information must be encrypted using approved encryption. Similarly, to prevent unauthorized disclosure such as unauthorised viewing of unattended facsimile equipment, employ the following measures:

(a) locate facsimile machines and image processing terminals within areas under physical access control;

(b) prohibit facsimile transmissions carrying official secret information, unless it is determined by independent means that a properly authorised person is present at the receiving terminal. One method of doing this is to send the cover sheet only, wait for telephonic acknowledgement of its receipt, then resend the entire package using the redial button on the facsimile device; and

(c) classify and label documents in image systems or those received via facsimile using the same criteria used for paper documents. Documents should bear markings appropriate to their classification.

Use secured cellular facsimile for transmission of official information

The use of secured cellular facsimile raises potential disclosure concerns. In protecting against disclosure of facsimile sent via secured cellular connections, prohibit transmission of official secret information through cellular facsimile unless encryption is in use.

3.4.3.5 Unsolicited Messages

Disclose facsimile number on a need-to know basis

Restrict the disclosure of encrypted facsimile machine numbers on a need-to-know basis. This will help reduce unsolicited messages and minimise service loss caused by junk facsimile.

3.4.3.6 Retention of Documents

Keep a copy of information on secured media

In order to prevent the loss and modification of necessary business records (including facsimile on thermal paper and stored image where source documents are not available), store image on secured media. It should then be stored, or a separate copy made, kept off-line and retained.

3.5 Electronic Mail

E-mail – an electronic communication over computer system

Electronic mail (e-mail) is the electronic communication over computer systems that enable two or more parties to send, receive, store and forward communications over public and private networks. Multiple message types may be transmitted such as text, digitised voice and images.

Within the public sector, there are two (2) categories of e-mail:

Categories of e-mail

(a) Official E-mail

Official e-mail is under the supervision and control of the Malaysian Government. Contents of the official e-mail can be categorised as:

i. non-classified official e-mail for handling unclassified official information by following the procedure issued from the respective ministry, department and agency; and

ii. classified official e-mail for handling classified official information that must be protected in the interest of the government.

(b) Personal E-mail

Personal e-mail is not under the supervision and control of the Malaysian Government. Personal e-mail cannot be used for official matters.

3.5.1 Authorised Users

Use logical and physical access control

Authorised access to e-mail facilities should be controlled. Employ both logical and physical access controls to ensure authorised access.

3.5.2 Physical Protection

E-mail physical protection

All ICT assets when taken together provide e-mail services should be protected from unauthorized users and to ensure service provision. Protective measures include:

(a) limit physical access to employees and or maintenance crew who are necessary for the operation of the system; and

(b) house ICT assets supplying e-mail services away from public areas.

3.5.3 Logical Protection

E-mail logical protection

In order to prevent unauthorised modification, disclosure or destruction of information residing in computer systems, logical access control for all computers must be applied.

3.5.4 Integrity of Content

E-mail integrity

E-mails can be the beginning of a series of actions to be taken. Before actions are initiated, it may be necessary to determine the integrity of its content. This is accomplished by:

(a) verifying the authenticity of source through telephone, facsimile or reply e-mail, or

(b) use of approved digital signature.

3.5.5 Disclosure

Protect against disclosure via e-mail systems

E-mails carrying official secret information must be protected against unauthorised disclosure via:

(a) label information that is classified as per *Arahan Keselamatan*;

(b) prohibit the transmission of official secret information over e-mail, unless encrypted using technique approved by government;

(c) all classified information must be kept encrypted; and

(d) forwarding of official secret information must be with prior permission from the document originator.

Minimising misdelivery

In order to minimise misdelivery:

(a) to avoid misdirection of official secret information and hence disclosure, re-check the receipient e-mail address and identify prior to encryption and sending. Attach appropriate warning messages to assist the receipient at the receiving end.

(b) receiver must acknowledge receipt of information;

(c) for bounced mail, prohibit retransmission until the cause is identified; and

(d) use trusted public network providers.

3.5.6 Message Retention

Messages should be stored and easily retrieved

Official e-mails are public records and should be treated as such. As with current paper based documents, e-mails should be stored into appropriate folders for easy retrieval and reference. There may also be cases where e-mails are stored for business and regulatory reasons. To assist in proper management of e-mails:

(a) create a record retention;

(b) purge unread and unsaved messages after a specified time; and

(c) handle all electronic records of archival value, in compliance with *Akta Arkib Negara Malaysia 44/1966*.

Public key certificates or authentication keys used during processing should be archived together with messages to ensure proper reconstruction and authentication.

3.5.7 Message Reception

Facility to confirm message status

Most e-mails of good repute offer function to allow users to manage their e-mail messages. Users may find it useful to use automated status checking facility to ensure all messages are received and read.

3.5.8 Protection against Malicious Code

Message should be free from malicous code

Messages sent and received via the mail system should be cleaned from malicious code by:

(a) scanning all files and attachment;

(b) not opening any attachment files from unknown or suspicious senders; and

(c) using the latest and up-dated anti-virus software.

3.5.9 Security Labelling

Message should be labelled as per *Arahan Keselamatan*

E-mails and its attachment containing official secret information must be given security labels as per *Arahan Keselamatan*.

3.6 Mass Storage Media

Storage media for vast quantity of information stored

Microfilm, microfiche, compact disk (CD), diskette, tape, cartridge and other mass storage media pose special concerns because of the vast quantity of information they can store, and the relative inability to readily ascertain their contents. Hence special precautionary measures have to be taken in order to ensure that the confidentiality, integrity and availability of the information contained within the storage media are intact and secured.

The following controls should be put in place:

3.6.1 Protection of Information in Storage Media

Information protection in storage media

In order to provide greater security of official secret information stored on magnetic media, the following steps have to be taken:

(a) encrypt all official secret information upon storage;

(b) physically protect the storage media from unauthorised access or removal;

(c) maintain a formal record of the authorised recipients of information;

(d) provide access restrictions and control to back-up files/copies activities; and

(e) index the media for identity with instructions on special handling, if required.

3.6.2 Environmental Considerations

Media are sensitive to environmental conditions. Storage site should be adequately provided with fire and environmental control

Mass storage media may have different sensitivities to environmental factors, and therefore require different measures of environmental protection. Magnetic media, such as diskettes or magnetic tapes are sensitive to temperature, liquids, magnetism, heat, smoke and dust.

In order to prevent destruction of information due to environmental problems, the storage sites should be provided with adequate fire protection and environmental control in accordance to the media's manufacturers' specifications.

3.6.3 Disposal of Storage Media

Disposal of unused storage media

Storage media should be disposed of securely and completely when it is no longer required, to prevent improper disclosure.

Formal procedures should be taken to minimise the risk of sensitive information leaking through careless disposal. The recommended procedures are as follows:

(a) media containing classified information should be disposed by shredding, grinding (granularising) or burning;

(b) use of the degaussing process as a recommended method to magnetically erase data from magnetic ICT media. Two types of degausser exist: strong permanent magnets and electric degausser; and

(c) disposal of sensitive items should be logged in order to maintain an audit trail.

When accumulating media for disposal, consideration should be given to the aggregation effect, which may cause a large quantity of unclassified information to become more sensitive.

3.6.4 Non-Current Storage Media

Non-current storage media should be transferred to the new media before disposal

In order to ensure availability of information stored on non-current storage media, the information should first be transferred to the new current storage media before deletion or disposal. However, should the organisation continue to utilise non-current storage media, care must be taken to retain all the necessary peripheral equipment such as its drivers, and ensure its working order.

3.6.5 Intellectual Property Rights

Compliance to Malaysian Copyright (Amendment) Act, 1997

Commercial software products are usually supplied under a license agreement that limits the use of the products to specified machines and may limit copying to the creation of back-up copies only. In preventing infringement of intellectual copyrights due to unauthorised copying of software on mass storage media, compliance to the Malaysian Copyright (Amendment)Act, 1997 must be ensured at all times.

3.6.6 Vendors, Contractors, External Service Providers, Third Party Access

Control access by Vendors, Contractors, External Service Providers and Third Party

Information is an asset and should be protected. Third party access to government documents for referral to perform a specific task should be controlled. For example, a new ICT system installation may require referral to blue prints, plans, migration forms, approvals etc.

Access to information including assets, facilities, and documents should be evaluated. This is to ensure acceptable risk by allowing third party access. The more sensitive the information is, the higher approval authority is required.

In the government environment, the authority level is specified clearly for the official secret information as described earlier. Government officers must strictly adhere to guidelines issued such as *Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Kerajaan Bil. 03 Tahun 2000* before allowing third party access.

3.7 Business Resumption

Business Resumption Plan for the Public Sector

Government ICT installations store huge amounts of information. This information is varied in nature, from information for daily functions to information for producing trends and analysis. The monetary value attached is of sizable amount. The content value of the information is immeasurable and in some instances may be difficult or if not impossible to reconstruct. Therefore all ICT installations should have some form of business resumption plan.

The plan should be geared towards achieving continued business operation. In instances where it becomes impossible to do so then the plan should target for continuous functioning of core operations. The activities involved in the business resumption are as follows:

(a) risk analysis;

(b) disaster recovery/contingency plan;

(c) regulatory compliance; and

(d) insurance.

3.7.1 Risk Analysis

Organisation Risk Analysis Model

The organisation's risk analysis involves analysis of background of risk, business impact, threat and vulnerability, protection, compliance, follow-up and feedback. These major components are essential for the analysis of risk. The organisation risk analysis model is illustrated in figure 3.2: Risk Analysis Model.

3.7.2 Disaster Recovery/Contingency Plan

Disaster Recovery/ Contingency Plan to ensure continuous functioning of critical business

The Disaster Recovery/Contingency Plan (DRP) forms an important part of the Public Sector ICT Security programme. As mentioned earlier, its objective should be to ensure continuous functioning of critical business in the event of disruption. The plan should outline roles and responsibilities in the event of a disaster or conditions that prevent continuous business functions. In addition, the disaster recovery plan should ensure that information and information processing facilities are restored as soon as possible after an interruption. Please refer to Appendix L of a Sample of Disaster Recovery and Contingency Planning.

The disaster recovery/contingency plan should include at least the following:

(a) a list of core activities considered critical preferably with priority rankings;

(b) a list of personnel available both internal and from the vendor together with their contact numbers (facsimile, phone and e-mail). Apart from that there should also be a second list to replace personnel who may be unable to attend to the incident;

(c) a detailed list of information that requires back-up and the exact location of storage as well as instructions on how to restore such information and related facilities;

(d) identification of alternative processing resources and locations available to replace crippled resources; and

(e) agreements with service providers for priority resumption of services where possible.

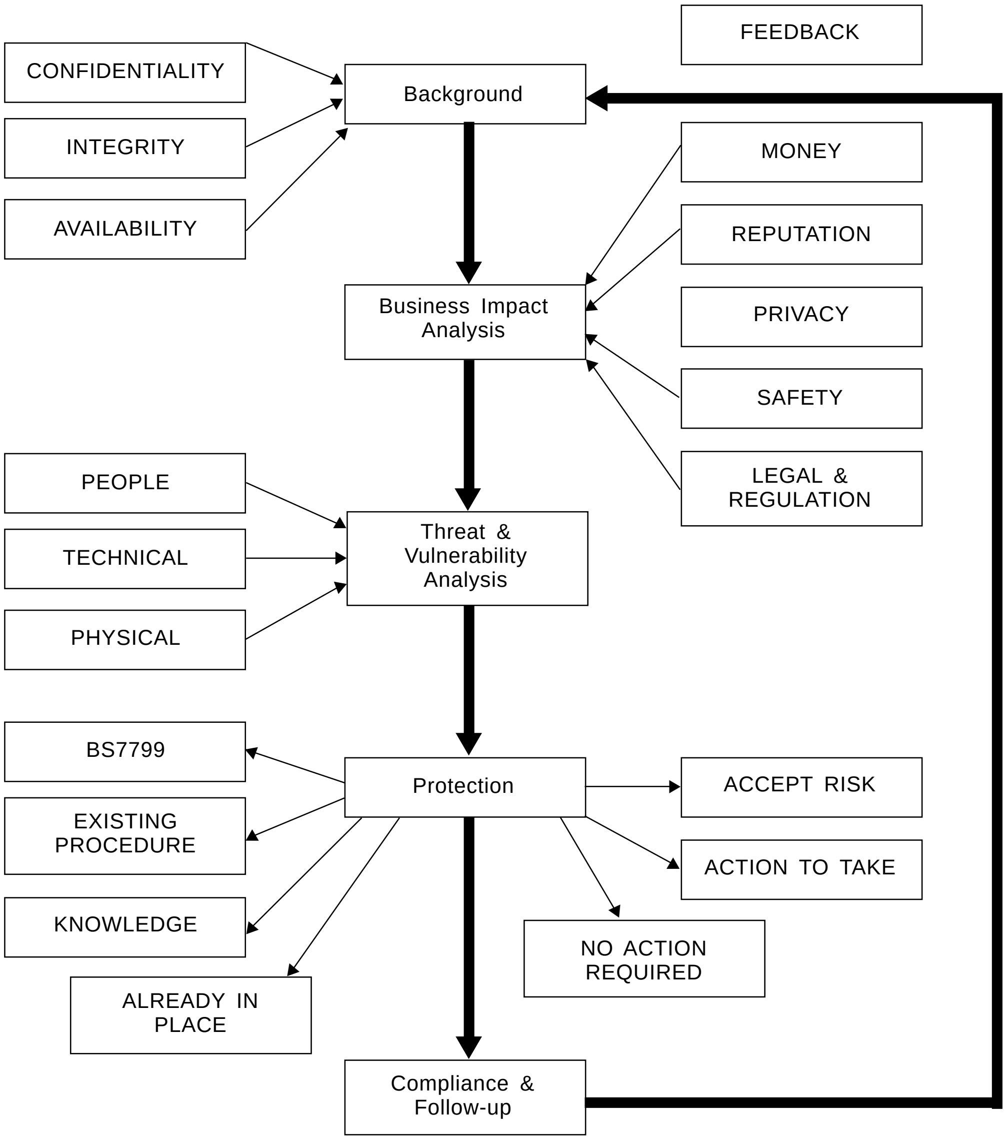


Figure 3.2: Risk Analysis Model

Source : NISER

Test the Disaster Recovery/Contingency Plan at least once a year

In order to ensure smooth transition, the disaster recovery/contingency plan should be tested yearly if not more. The testing of the plan has the added advantage of keeping the personnel trained and skills fine-tuned as well as identifying likely operational problems. The plan should also be evaluated periodically to ascertain that it is still appropriate and meeting the purpose it was intended for.

In ensuring against business interruption, recommended actions under the disaster recovery/contingency plan are:

(a) include telephone and voice mail service continuation to ensure the continued availability of voice mail and telephone services;

(b) include image systems and facsimile capability to ensure against business interruption due to loss of image systems;

(c) include e-mail service continuation to ensure business continuation in case of loss of e-mail services;

(d) continued availability of information stored on microfilm, microfiche, or other mass storage media should be ensured through the following procedures:

   i. include mass storage media, as part of the contingency and disaster recovery plan;

   ii. provide for back-up of all important files, critical business data, important programmes and documentation to enable business resumption of core processes;

   iii. the frequency of back-up should be in-line with the importance of the information and the business resumption plan;

   iv. back-up should be securely stored, and the recovery procedure checked and tested regularly for reliability; and

   v. access to back-up should be strictly controlled.

(e) include paper documents and media storage to ensure that vital business records are not lost through destruction or loss of paper documents;

(f) protect government operations from disastrous effects of fire and/or water:

   i. a business continuity or resumption plan should be in place and fully tested; and

   ii. back-ups of all important information, services and resources should be available.

(g) protect buildings containing key equipment and the key equipment against the effects of lightning; and

(h) protect against natural disasters by avoiding disaster prone areas.

3.8 Public Sector ICT Security Incident Handling

A security incident affects confidentiality, integrity, availability and accountability

A security incident is an incident that affects either directly or indirectly, the confidentiality, integrity and availability of the ICT system.

Incident handling is similar to first-aid. Once an organisation suffers a disruption and is given an ‘incident handling’, where its ICT infrastructure needs to undergo a proper overall security diagnosis.

3.8.1 Causes of Security Incidents

Many causes of security handling

There are many causes of security incidents either:-

(a) intentional such as virus, deliberate attacks, sabotage etc; and

(b) unintentional such as programme errors, technical deficiencies, lapses in responsibility etc.

More common these days are events caused by deliberate technical activities internally or externally launched by hackers.

3.8.2 Handling Security Incidents

Security incident handling procedure

Following a security incident, the computer manager or ICTSO will be required to take necessary measures to minimise the resulting damage or those which may be required by law:

(a) order the security incident handling team of the organisation (if it has been set up) to look into the matter immediately;

(b) report the incident to Government Computer Emergency Response Team (GCERT), MAMPU and seek further advice as per requirements of the *Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) - Pekeliling Am Bil 1 Tahun 2001*; and/or

(c) report to respective agencies such as the police within 24 hours. [Refer to Appendix H for further advice]

3.8.3 Developing Security Incident Handling Capability

Characteristics of security incident handling

Characteristics of successful incident handling capability:

(a) Good Understanding of the Domain.

‘Domain’ means all relevant programmes and users affected by the anticipated incident. In a networked environment, an incident handling capability may define that its constituency to cover only a particular single Local Area Network (LAN) environment which is considered to be critical and cost justifiable. Certainly, if the domain coverage is as wide as the entire organisation, then the ‘understanding’ to be developed needs to cover the entire organisation;

(b) High-level Awareness

Users need to be aware of the importance of incidents handling, and to trust its capability. High-level awareness can be achieved through good and effective security training programmes. Users can play a significant role in recognising threats, reporting and providing preliminary emergency response;

(c) Centralised Reporting and Communications

All suspected security incidences must be reported to the ICTSO immediately. The ICTSO should then report to the CIO. Based on the gravity of the incident, the ICTSO may proceed to seek technical advice from MAMPU; and *(d)* Competent Technical Support

In selecting members of the incident handling team, the following should be considered:

i. expertise in Public Sector ICT Security;

ii. ability to work as a team;

iii. effective communication between all parties from unskilled users to managers to law enforcement officers (police);

iv. reachable on call 24 hours X 7 days;

v. available on short notice; and

vi. ability to liaise with other organisations effectively.

Benefits of security incident handling capability

Benefits of an internal ICT Security incident handling capability;

(a) Limit Damage from an Incident

Such a capability enables users to report incidents promptly and the organisation to quickly provide appropriate response and assistance. This includes establishing contacts with supportive sources (technical, managerial, legal and security) to help in containing and recovering from the incident;

(b) Prevent Future Recurrence

When an incident occurs, the problem can be studied so that more effective safeguards can be implemented. Additionally, through outside contacts, early warnings can be provided and this tends to stop the problem from spreading;

(c) Identify Other Threats and Vulnerabilities

An incident handling can greatly facilitate analysis of future threats by exploiting information logged due to the incident. This helps to identify potential recurring problems;

(d) Enhancing Internal Communications and Organisation Preparedness

A crisis will encourage communication between members of the organisation to respond to any type of future incidents (not just security-related incident). It will also serve to maintain good relation between the organisation and other relevant agencies; and

(e) Enhancing Security Training and Awareness Programme

Based on incidents reported, training personnel will have a better understanding of user's knowledge and awareness of security issues. Citing actual events in training, results in better response.

Liaison with other organisations

Since computers are networked, incident occurring in one organisation may affect other organisations. Thus, there is a need to liaise with other teams in other organisations, perhaps even pooling knowledge via an e-mail group.

Support from technical team

A good technical team needs to be identified and trained to handle security incidents successfully. Otherwise the task has to be outsourced.

Immediate team action is facilitated by the establishment of a centralised reporting mechanism

Rapid team action is facilitated by the establishment of a centralised reporting mechanism. When the incident involves an organisation that handles national security, the means of communication must also be secure, for example using approved encryption for voice, facsimile or e-mail.

3.8.4 Issues to Consider When Setting an Incident Handling Capability

There are several issues that should be considered in setting an incident handling capability. These are:

Start up issues

(a) Set-up Cost;

(b) User's Perception;

(c) Personnel;

A minimum set of personnel listed in the plan includes a computer manager and at least one technical staff.

(d) Demography of the Organisation; and

Should the incident handling require travel to distributed sites, there should be funds allocated for this. Some organisations may also have branches overseas.

(e) Security Awareness and Training.

There will be requirements for initial training and continuous education on latest developments in Public Sector ICT Security. An associated issue will be the budget for seminars, workshops, conferences and continuous education programmes. It cannot be emphasised further how a good incident handling capability is closely related to an organisation's training and awareness programme. Users will be educated about such incidents and what to do when they actually occur. This can increase the likelihood that incidents will be reported early, thus minimising the damage.

3.9 Public Sector ICT Security Awareness, Training, Acculturation and Education

Allocate sufficient resources for planning and implementing Public Sector ICT Security awareness, training, acculturation and education programmes

ICT systems are as good as the people that operate them. Though application and sensitivity may differ amongst government departments the people is usually regarded as one of the weakest links in attempting to secure ICT systems. Therefore it is of the utmost importance to allocate sufficient resources for the planning and implementation of programmes on Public Sector ICT Security awareness, training, acculturation and education.

Security conscious and trained employees are able to improve ICT security systems

Security conscious and properly trained employees are still one of the best means to improve any Public Sector ICT Security system. Programmes that are conducted properly will make employees realise the importance of their role in ensuring the safety of their ICT environment. Therefore the Public Sector ICT Security awareness, training, acculturation and education programmes should be designed such that it enhances security from both the assets and human counterpart point of view.

Copyright MAMPU

This is performed by:

(a) Improving Awareness

Often the biggest challenge towards making a start in Public Sector ICT Security. Users should be exposed to Public Sector ICT Security issues to bond a common interest in the need to protect ICT systems. By making users aware of their responsibilities, they then become accountable for all their actions or inactions in lapses of security. Teaching users the correct ICT security practices (for example to avoid short cuts) helps mould user behaviour. It also supports individual accountability, which is one of the most important means of improving Public Sector ICT Security;

(b) Developing Skills and Knowledge

To enable users to perform or to take remedial actions in a more informed manner. Users tend to behave predictably once they become aware of the consequences of their actions. Skills development and knowledge upgrade has always been looked upon as a requirement for users to perform their jobs in an explained and secure manner. This requires a conscious and concerted effort from management; and

(c) Building In-depth Knowledge

Since threats are becoming more sophisticated, varied and sometimes identifiable only at the end of an attack, there is always the need to keep abreast with technology, defence mechanisms, methodologies, case studies etc as needed for the design and implementation of Public Sector ICT Security programmes.

3.9.1 Benefits of Public Sector ICT Security Awareness, Training, Acculturation and Education

Benefits of ICT security awareness, training, acculturation and education

The benefits of the Public Sector ICT Security awareness, training, acculturation and education programmes are as follows:

(a) the formalisation of the Public Sector ICT Security programmes should indicate the seriousness of the government in protecting its ICT assets. By understanding Public Sector ICT Security issues, employees are able to improve on their behaviour as they become more equipped and able to exercise best practices; and

(b) Heads of Department on the other hand are able to hold their staff accountable for all their actions or inactions and they would now not be able to plead ignorance.

Awareness stage which is followed by training, programme, enforcement and follow-up

The awareness stage can be followed by a training programme, such as identifying vulnerabilities and implementing safeguards. Once the training has been conducted, the enforcement and follow-up can follow suit. At this stage, it would be difficult for employees to provide convincing argument when caught doing something wrong.

Accordingly, the government adopts the principle of accountability as a basis of the Public Sector ICT Security Policy where all users are made accountable for all their actions or inactions. It is recommended that user accountability be stated clearly and prominently in accordance to the sensitivity of information accessed. To ensure that the responsibility is discharged, the government requires that ICT systems possess capabilities that can track user activities.

3.9.2 Public Sector ICT Security Awareness

Importance of ICT Security practices

Due to the huge repositories kept and the ingenuity to translate system weakness into gains, it has become necessary to remind those being trained about Public Sector ICT Security the importance of sound Public Sector ICT Security practices.

Explaining the consequences of Public Sector ICT Security failure in terms of effects to the organisation (embarrassment, monetary value, recovery efforts and time loss) and the preventive measures that should have been taken, should provide enough motivation to protect ICT assets.

Users are trained based on the level and job function

There are many types of users of government ICT assets. The awareness programme to be developed should consider the various roles to be extracted and expectations of these different user groups. For example, for those in management, the awareness programme could be designed towards managing the roles of establishing Public Sector ICT Security.

As for other groups such as those in the technical environment, the awareness programme should be geared towards Public Sector ICT Security relating to their actual jobs in processing, dissemination or report generation. In today's environment where almost everyone in the public sector has access to ICT resources, the awareness should consider the different educational backgrounds, job specifications and security clearance in deriving the maximum benefits for all target groups.

	AWARENESS	**TRAINING & ACCULTURATION**	**EDUCATION**
Attribute :	'What'	'How'	'Why'
Level :	Information	Knowledge	Insight
Objective :	Recognition	Skill & Experience	Understanding
Teaching Method :	Media : - Video - Newsletter - Posters - Lecture - Class room - Seminar	Practical Instruction - Lecture - Case study & workshop - Hands-on practice - Counselling	Theoretical Instruction - Discussion - Seminar - Background reading - Class room
Test Measures :	- Understanding - Interview - Case study	- Problem Solving (applied learning) - accreditation	Essay (interpret learning)
Impact Time Frame :	Short-term	Intermediate	Long-term

Table 3.2: Public Sector ICT Security Awareness, Training and Education Programme

Every employee has a role in ensuring and protecting ICT resources

The awareness programme should be designed to reinforce the importance of Public Sector ICT Security and the fact that every one in the civil service especially those who have access to ICT assets, have a role in ensuring and protecting ICT resources. Should employees fail to realise this or should they view Public Sector ICT Security as just another set of rules and procedures, they may end up becoming passive passengers. It is also advantageous that when awareness programmes are conducted, active participation is always encouraged so that views on security threats and vulnerabilities could then be used as input to improve Public Sector ICT Security.

Topics to be covered in the awareness programme

The awareness programme is also used to remind everyone of basic security practices such as the clear desk policy, need-to-know principle, proper log-outs and accountability. Thus it is recommended that governments department conduct regular Public Sector ICT Security awareness programme to cover suggested topics as follows:

(a) threats and vulnerabilities;

(b) impact of disclosure;

(c) roles and responsibilities;

(d) punitive actions; and

(e) abnormal events.

The list presented above may be expanded by the ICTSO when conducting such programmes.

Examples of media to be used to conduct the awareness programme

In conducting the ICT awareness programme it is also recommended that relevant information be used and conveyed through the use of multiple media such as:

(a) presentation papers;

(b) pamphlets, flyers and posters;

(c) films, videos, slides;

(d) CDs; and

(e) video conferencing.

3.9.2.1 Techniques

Awareness techniques

Established fora such as presentations, seminars, workshops, meetings, talks, lectures, demonstrations, and bulletin boards whether formal or informal should be used. It is also best to incorporate Public Sector ICT Security awareness into basic ICT training either at the point of recruitment or through scheduled training programmes. It is to be noted that no matter how well the awareness programme is designed, it may be neglected over time. For this reason the design of such a programme in terms of techniques and reach should be creative and flexible.

Awareness sessions are conducted via classes

In cases where the awareness programme is conducted through a classroom approach, it could be arranged either on a stand-alone basis or as part of another programme. The medium could be lecture-based, computer-assisted, multimedia-based or a combination of all three. It is also best to include case studies and a hands-on approach in designing such programmes.

3.9.3 Public Sector ICT Security Training & Acculturation

ICT training & acculturation should be designed with the purpose of imparting skills

Different from Public Sector ICT Security awareness, the Public Sector ICT Security training & acculturation should be designed with the sole purpose of imparting the necessary skills to users. Armed with the new skill sets, they should be able to perform their jobs more effectively. This includes a list of what they should or should not do and how they can go about doing it. There are however many levels of Public Sector ICT Security to be addressed depending on the sensitivity of the installation to be protected. It ranges from basic Public Sector ICT Security skills to the intermediate level or advanced and specialized skills. It can also be specific to particular ICT systems or generic to address common ICT issues.

In order to be effective, the training and acculturation programme should focus on the specific audience or be related to particular job skills. This is to ensure that the right people receive the correct skills to enable them to perform effectively. Under this topic there are two types of users that can be targeted:

(a) general users; and

(b) specialised or advanced skills users.

3.9.3.1 General Users

General users

This constitutes the majority of users who need to understand good Public Sector ICT Security practices such as:

(a) physical security e.g. protecting the perimeter, power supply, access control, environmental control, fire hazards, flood, etc;

(b) access security e.g. keeping access codes confidential, authorised versus unauthorised access, etc; and

(c) reporting responsibilities such as having knowledge of Public Sector ICT Security violations, virus incidents and any other form of untoward or unexplained incidents.

All users shall be formally advised by the respective departments regarding:

(a) individual access control, stating privileges based on current job functions; and

(b) the fact that ICT resources that they are privy to, belong to the government including the resources itself, data, stated information or information that is derived. The government reserves the right to monitor activities of all users accessing government ICT resources for misuse or use of ICT resources other than the purposes for which they were intended.

In designing training programmes, care should be exercised not to overload general users with unnecessary details. This is because the very same people are already the target for other training and acculturation programmes. It is best to focus on Public Sector ICT Security issues that affect the general users directly so that they remain alert to activities that affect them. For this group of users, the intention is to improve basic Public Sector ICT Security practices and not to make them experts on Public Sector ICT Security philosophy.

3.9.3.2 Specialised or Advanced Skills Users

Specialised or advanced skills

Apart from the general users, there is a small group within the public service that will require specialised or advanced ICT training on the technical and financial aspects of the ICT technology, specialised security products and specific mitigation efforts on security breaches. This group will include ICTSO, ICT officers and some senior members of management.

The identification of officers requiring specialised training can be done through various means often with the overriding objective to support and complement organisational goals.

One method is to identify new skill sets that would be required as a result of changes in requirements. For example, when organisations switch from mainframes to client server systems, it will cause a radical change to the system architecture hence affecting Public Sector ICT Security. Another method is to look at the job categories and job functions to identify skills needing upgrades. The management of skills upgrade, training and new skill opportunities is important to ensure the continuous supply of trained and competent human resource in ICT security. However, this function is often conducted haphazardly.

3.9.4 Public Sector ICT Security Education

Education training towards re-skilling and upgrading the skills

The ICT education programme offers a more structured approach towards re-skilling and skills upgrade in Public Sector ICT Security. It is normally targeted for ICTSOs or those whose job requires specific Public Sector ICT Security expertise.

3.9.5 Implementation

Implementation approaches

In order to ensure an effective Public Sector ICT Security awareness, training and acculturation, it is necessary from the very onset to have proper planning, execution and feedback. There are many approaches that could be used, one of which is outlined below consisting of seven major steps:

(a) understand the core business of the organisation;

(b) identify gaps in Public Sector ICT Security knowledge;

(c) align skill gaps so as to support the organisation's core business;

(d) identify suitable staff;

(e) secure financial resources and identify training locations; and

(f) execute, maintain and evaluate programme effectiveness.

3.9.5.1 Understand the Core Business of the Organisation

Identification of core business will assist in the design of the educational programme

The identification of the core business of an organisation will indicate the nature of the training programme that should be designed and implemented. The underlying factor is that the training programme to be embarked upon should support the goals and objectives of the organisation. From here onwards it would be easier to determine the scope of the training programme, which may include training for the entire hierarchy or limited to groups. Since training requirements differ, the training programme may need to be tailored accordingly or supplemented by more specific programmes.

The aim is to ensure ICT assets are protected at an acceptable level

The overall aim of the ICT education programme is to ensure that ICT assets are accorded the appropriate level of protection by increasing awareness towards Public Sector ICT Security.

3.9.5.2 Identify Gaps in Public Sector ICT Security Knowledge

The aim is to bridge existing gaps

The purpose of this exercise is primarily to bridge existing gaps in Public Sector ICT Security knowledge pertinent to the organisation. It also helps to reinforce and build upon basic knowledge already available amongst members. Should this not be done, the organisation runs the risk of sending people to the same course resulting in waste.

3.9.5.3 Align Skill Gaps to Support the Organisation's Core Business

The aim is to determine the education programme support organisational needs

This is also an important aspect in determining that the education programme support organisational needs. One method of achieving this task is to list all skills currently available and comparing it with the list of skills necessary to support the mission of the organisation. In doing so the skill gaps become apparent and should be prioritised accordingly.

3.9.5.4 Identify Suitable Staffs

The aim is to identify the level of skill

There are many levels of ICT training, each level being suitable to the different categories of staff within the organisation. At the beginning it may not be possible to meet all the training needs, thus it is suggested that the identification of staff eligible for training be segmented according to:

(a) Level of Public Sector ICT Security Knowledge

The target audience may be grouped according to its current level of Public Sector ICT Security knowledge. This may require some research to determine the individual skill level. For the ICT expert, a highly technical training programme is more suited than one that touches on management issues or Public Sector ICT Security fundamentals. The same can be said for a new recruit who will find difficulty in understanding highly technical issues;

(b) Job Task or Function

Target audiences may be grouped according to their job task or function such as data entry, operations, maintenance, general users, management or network specialists;

(c) Job Category

Different job categories generally carry different responsibilities whereby the Public Sector ICT Security training requirement will also be different. Some examples are application development, systems design, and systems testing; and

(d) Types of ICT Systems Used

Public Sector ICT Security measures vary according to platforms and applications. It may be necessary to design security training programmes that meet specific requirements of the installation.

3.9.5.5 Allocate Financial Resources and Identify Training Location

Training programme should be identified during budget

Training programmes can be a drain on financial resources especially for courses that are only available overseas. There may also be a time lag between the availability of funds and training dates. Currently in the public sector, for budgetary purposes, the planning to secure financial resources takes place once in two (2) years before the training programme starts.

In identifying training locations, departments are required to give preference to courses provided by recognized or reputable ICT training organisations. In doing so the course topics, content, methodology, approach, materials, courseware, etc can be assured to be of use and beneficial to the participants.

3.9.5.6 Execute, Maintain and Evaluate Programme Effectiveness

Training programme should be executed, maintained and evaluated for effectiveness

A training programme no matter how comprehensive will remain a training programme unless it is executed, maintained and evaluated for effectiveness. In terms of Public Sector ICT Security, the training programme should be visible so there is constant awareness of its existence. The visibility creates awareness signalling a high sense of anticipation. Users on the other hand realise that improper conduct could soon come to an end. In many instances, ICT training programme announcements create a receptive learning mode.

The methods used should include instructor-led sessions with consistent materials presented and tailored to the needs of the target audience. It could exist as a stand-alone, one time training or a series of training with gradual increase in subject matter. Apart from this, it could be useful to have a mix of classroom with hands-on training and exam.

ICT technology changes so rapidly that it is possible to expect new technologies in the market every two months. There should be planned effort to keep abreast of changes in the ICT technology especially those that affect security requirements.

It is possible that approved training programme needs may become irrelevant when an organisation uses new applications or effects changes to its environment. A good example is when an organisation switches to Internet technology thus renders existing security guidelines useless. Similarly a training programme can become outdated when there are changes in policies and laws. Before the advent of e-mail, the government's official communications was through letters, telephones and later facsimiles. With e-mail, new guidelines need to be established to regulate its use and to ascertain integrity and point of origin. Therefore in light of the inevitable changes brought about by either technology or changes in policies/laws, training programmes too should reflect such changes.

Measure training programme

Similar to other training programmes, the effectiveness of security training is not easy to measure. Nevertheless, some form of measurement must be made in order to justify resources spent. Indicators such as retention of information and adherence to security procedures do indicate a certain degree of effectiveness.

Organisation could also employ proven programme measurement indicators such as:

(a) Participant's evaluation of courses/programmes;

(b) monitor Public Sector ICT Security incidents before and after training; and

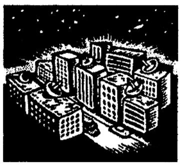
(c) use of 'cascade effect' by requiring returning participants to demonstrate skills and understanding.

Copyright MAMPU

More often, the training on Public Sector ICT Security occurs as an after thought. As threats and vulnerabilities become more sophisticated, liberalisation of the Internet added further exposure to practically all ICT resources. It is common knowledge that ICT attacks could be mounted from anywhere within a short time frame and all evidence removed in an equally short time. There is therefore an urgent need to match disruptive capabilities with superior on-going counter measures.

3.10 Physical and Environmental ICT-Security

Approval from the Chief Government Security Officer for all physical and environmental-related issues



In order to prevent unauthorised access, damage and interference to premises and information, all proposals related to buildings, acquisition, lease, renovation, purchase of government and private buildings housing information processing facilities have to be referred to the Chief Government Security Officer. The physical protection provided should commensurate with the identified risk and be based on the principle of defence-in-depth.

3.10.1 Physical Security Perimeter

Physical security perimeter should be considered to provide physical barriers around the premises

The physical strengthening of information processing facility is necessary to deter potential intruders. Multiple physical barriers that surround premises housing information facilities help to deter, detect and delay intruders. Where appropriate:

(a) clearly identify the perimeter to be secured;

(b) identify physical vulnerabilities and weaknesses by conducting risk analysis;

(c) ensure that the perimeter walls are physically sound and entrance into the perimeter area is only through doors equipped with suitable access mechanisms;

(d) use of real floor and real ceiling such that physical threats is seen and not hidden;

(e) control access by means such as registration counter, smart cards, camera etc; and

(f) alarms to detect excessive smoke, heat, moisture and unauthorized entry

3.10.2 Physical Entry Controls

Secure areas should be protected

Once areas are gazetted as Secure Areas, these areas are accorded suitable protection so as to allow legitimate access. The following controls should be considered.

(a) visitors should be escorted until “handed over” to their change and details of their entry and exit duly recorded. For some installations, visitors are accepted by appointment only with predetermined routes and access privileges;

(b) for unmanned counters, use identification tags that doubles as door access control;

(c) allow access to ICT assets and passageway to authorised employees only;

(d) authorised employees and visitors to use clearly identifiable tags so as to differentiate and to quickly identify trespassers;

(e) review access rights to secure areas regularly to reflect changes in function, job description etc; and

(f) Chief Government Security Officer advice on secure door locks and related access control services.

3.10.3 Secure Area

Secured area – area where access is restricted and limited to authorised employees only

A secure area may be defined as an area where access is restricted and limited to authorized employees only. This is done to protect the contents that are housed in the area. Department heads in consultation with the ICTSO is required to review the security requirements of their installation and plan for the provision of suitable protection within the secure area and its immediate surroundings. Consideration should also encompass relevant health and safety regulations. Reference should also be made to the Chief Government Security Officer to determine whether to gazette the secure area.

Preventive steps required to be taken to prevent unauthorized access include all or part of the controls below:

(a) limit the entrance and exit points;

(b) erect gates/grills and install security lighting;

(c) employ security guards equipped with suitable security tools;

(d) locate secure areas away from public passageway;

(e) secure areas to be bereft of markings, signs or any indication to betray its importance;

(f) secure areas should use doors that slam shut after opening or leave an audible warning when left open for an unreasonable duration;

(g) secure areas should be manned where possible with random patrols. When left unattended, all exits, entrances and windows should be locked;

(h) install intruder detection systems such as cctv and silent alarms linked to a command control center; and

(i) treat information, no matter how trivial emanating from secure areas as confidential and employ need to know principle.

3.10.4 Working in a Secure Area

Working protocols in secure areas

Employees and third party personnel may work in a secure area. As such, control mechanisms should be emplaced to prevent any untoward incident.

The following should be considered:

(a) escort third party personnel at all times;

(b) provide separate working areas for employees and third party personnel;

(c) halt all production work within secure areas when in the presence of authorized guest(s);

(d) all work within secure areas should be supervised;

(e) information about work within secure areas is on a need to know basis; and

(f) control movement, transfer, introduction or removal of equipment.

3.10.5 Site Protection for Data Centre and Computer Room

Data Centre and Computer Room should be secured

The following site design guidelines and controls should be considered and implemented where appropriate:

(a) the site shall not be in a location that is vulnerable to natural or man-made disaster e.g. flood, fire, explosion etc. Relevant health and safety regulations, standards and also any security threats presented by neighbouring premises should be taken into account;

(b) the site should be made as inconspicuous as possible to give minimum indication of its purpose;

(c) locations of computer facilities should not be identified;

(d) hazardous and combustible materials should be stored securely at a safe distance from the site;

(e) main fallback equipment and back-up media should be at a safe distance to avoid simultaneous damage;

(f) safety equipment should be checked regularly;

(g) emergency procedures should be documented and tested regularly;

(h) doors and windows should be locked at all times and external protection should be considered for windows; and

(i) external wall of site should be of solid construction.

3.10.6 Equipment Protection

In order to ensure all equipment are secured accordingly and are fully functional, the following equipment protection guidelines and controls should be considered:

3.10.6.1 Hardware Protection

It is important to ensure that all hardware are secured, operating and functioning well.

3.10.6.2 Storage Media Protection

Physical and environmental protection for storage media

In order to ensure the safety of official information stored on mass storage media, the following procedures need to be applied:

(a) designate a special restricted area for storage of mass storage media containing official information. As such, the restricted area would be accorded suitable physical protection;

(b) provide special storage facilities approved by Chief Government Security Officer such as protective cabinets or other securable storage facilities for media containing official information. This facility should protect its contents against unauthorised access and/or the effects of natural disasters such as fire or floods and harmful substances (e.g. dust).

(c) restrict access to the secure storage location; and

(d) document all procedures and access authorisation levels.

In preventing unauthorised removal, destruction or disclosure of information, the following management procedures are recommended:

(a) provide access restriction and control to all areas containing a concentration of information storage media. In addition, consideration should be given to the use of electronic article surveillance security systems;

(b) all media should be stored in a safe, secure environment, in accordance with the manufacturers' specifications;

(c) logging of all accesses made to the media should be established to support accountability;

(d) provide automated media tracking systems for maintaining inventories of storage media libraries; and

(e) authorisation for the removal of information should be required from the organisation and a record of all such removals should be kept.

3.10.6.3 Documentation Protection

In ensuring that documentation is not open to unauthorised access, consider the following steps:

(a) store/lock safely and securely;

(b) use physical or electronic security label;

(c) use encryption software for classified document;

(d) handle properly movement of classified document; and

(e) for secure handling of paper documents, refer to *Arahan Keselamatan*.

3.10.6.4 Cabling Protection

Cables need to be protected

In protecting cables from interception, damage and overloading, consider the following:

(a) cabling should be physically protected against accidental or deliberate damage;

(b) select cable type appropriate to its purpose;

(c) plan carefully by taking into account future developments; and

(d) cables should be protected against wiretapping.

3.10.7 Environmental Security

In order to ensure environmental security, proper functioning of critical and sensitive information processing facilities must be given due consideration.

3.10.7.1 Environmental Control

Power supply should be suitable and air conditioning should be controlled

The following guidelines should be considered:

(a) plan carefully the layout of the data centre (console room, printing room, partitioning of computer equipment, etc);

(b) control room temperature and humidity accordingly;

(c) provide adequate ventilation for work areas;

(d) provide suitable eye and nose protection appliances;

(e) printing rooms should be separate from computer equipments; and

(f) use raised flooring in the data centre.

3.10.7.2 Power Supply

All ICT equipment should be protected from power failure. A suitable power supply should be provided including uninterruptible power supply, if necessary. The use of a stand-by generator is required for critical data centres.

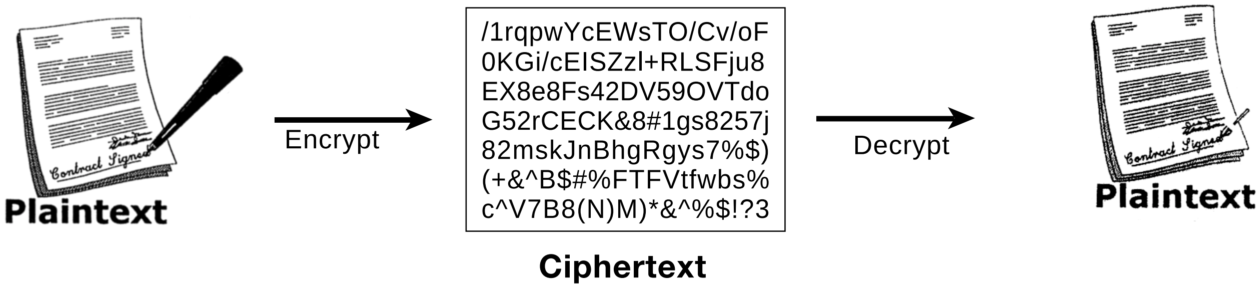
3.10.7.3 Emergency Procedures

Emergency procedures should be established, documented and posted at key locations. It should be tested at least once a year.

3.11 Cryptography

What is cryptography

Cryptography which is traditionally known, as the art of 'secret writing' is a branch of mathematics based on the transformation of data. The transformation process is called encryption. When encrypted, a plaintext becomes unintelligible and the unintelligible version is called a cipher text. In order to recover the initial plaintext, the cipher text must be subjected to a reverse process called decryption. Both encryption and decryption are done using a key.



Importance of cryptography to ICT security

Today, cryptography is the most important and fundamental tool to manage ICT security. Its usage is found in almost all aspects where security is of concern. This is more than just for keeping secrets (confidentiality), but also data integrity, digital signature and advanced user authentication.

Encryption is only part of the total solution

Although modern cryptography relies upon advanced mathematics, a typical user can still reap its benefits without understanding the heavy mathematics. Nevertheless, there are important issues to be considered when incorporating cryptography into computer systems. This is because any security solution should be seen in totality. Employing strong encryption may still not solve a problem because break-ins are made through other weaknesses and vulnerabilities.

Cryptography consists of algorithm and key

Basically, cryptography relies upon two components namely an algorithm and a key. In modern cryptographic systems, algorithms are complex mathematical formulae and keys are strings of bits. For two parties to communicate, they must use the same algorithm (or algorithms which are designed to work together). In some cases they must also use the same key. Such keys are normally kept secret. There are also situations in which even the algorithms need to be kept secret.

Two types of cryptography systems: symmetric and asymmetric

There are two types of cryptographic systems: symmetric and asymmetric. A symmetric cryptosystem (also known as secret-key cryptosystem) uses the same key to encrypt and decrypt a message, while an asymmetric cryptosystem (also known as public-key cryptosystem) uses one key to encrypt a message and a different key (the private key) to decrypt it.

Comparison between symmetric and asymmetric systems

Both types of systems have different features and offer advantages and disadvantages. Although they can be differentiated, comparing them is like comparing an apple with an orange. For example, symmetric systems are generally faster and require only a single key, whereas asymmetric systems are slower and need two keys. However, key distribution is a major problem for symmetric systems, yet it is not so in the asymmetric systems. Often, they are combined to form a hybrid system to exploit the strength of each type. In determining which system to use, an organisation needs to identify its security requirements and operating environment. An appropriate policy should be developed.

3.11.1 Symmetric (or Secret) Key Systems

In symmetric system, key privacy is most important

In symmetric key systems, two or more parties share the same key, which is used to encrypt and decrypt data. Here, the security hinges on maintaining the key secret. If the key is compromised, the security offered is severely reduced or eliminated. In this type of system, it is assumed that all members who share the same key do not disclose it and are responsible to protect it against disclosure.

The best known symmetric key system is the now unused Data Encryption Standard (DES). It was recommended as a standard by NIST, United States until it was shown in the early 90’s to be breakable.

Main problem with symmetric system is secure key distribution

Symmetric cryptosystems have a problem: how to transport the secret key from the sender to the recipient securely and in a tamper-proof fashion? Frequently, trusted couriers are used as a solution to this problem. Examples of symmetric key systems include 3DES (which reuses the DES 3 times), IDEA, RC5, Twofish and Rijndael. Another, more efficient and reliable solution is to rely on an asymmetric key system.

3.11.2 Asymmetric (or Public) Key Systems

Asymmetric system is designed to address key management problem

Since a secure cryptographic system requires the periodic changing of an encryption key, key management becomes a significant problem. Asymmetric or public-key encryption which was developed in 1976 addresses this problem. A public key encryption algorithm uses different keys for encrypting and decrypting information. Information encoded with either of the keys can only be decoded with the other key. It cannot be decoded with the same key. These two keys are created together and form a key pair. One of these keys is kept secret by the owner and is known as the private key. The other key, known as the public key, can be published widely. The relationship between the keys is such that it is extremely difficult (impossible for all practical purposes) to derive one key from the other.

In a public key system, there is no need for the sender and receiver to share the private key. It is only the public key that is distributed. In other words, the private key is never shared. Confidential messages can be sent using only the public key, and the decryption process requires the private key that is held just by the intended recipient. A further, very significant benefit is that public-key encryption can be used not only to ensure confidentiality, but also for authentication and digital signature.

Examples of asymmetric key systems include RSA (due to the designers Rivest-Shamir-Adleman), Digital Signature Standard (DSS), and ElGamal.

Minimum key length is 1024 bits

The minimum key length for encryption to be used in the public sector is 1024 bits and the cryptographic algorithm approved by the government.

3.11.3 Key Management Issues

Keys need to the managed properly to maintain integrity

The importance of looking after the cryptographic keys has raised many issues. The way they are created, distributed and used is critical to the confidence placed upon the cryptographic system. It is vital that there are well understood processes for:

(a) generation of new keys : users to be able to obtain suitable pairs of public and private keys;

(b) publication of the public keys;

(c) verification of the owner of a public key;

(d) determining the validity period of a pair of keys; and

(e) dealing with private keys that are lost or that may have been compromised.

Today the commonly accepted way to deal with the verification of public keys is through the use of certificates. A certificate is an electronic document that verifies the claim that a particular public key does in fact belong to a given individual (or organisation).

3.11.4 Disaster Cryptography and Cryptographic Disasters

When a disaster strikes, (see also Section 3.7.2 - Disaster Recovery/Contigency Plan), ICT components that use cryptography will require special handling. The situations are generally called disaster cryptography and cryptographic disaster.

3.11.4.1 Disaster Cryptography

Disaster cryptography is when disaster affects a cryptography

A ‘disaster cryptography’ means a situation when disaster affects cryptosystems and its uses. For a typical ICT component, recovery from disaster may entail a simple recovery using back-up and the person who is directed to perform the recovery may be allowed to read and access the components. However, for components which use cryptography, the procedure is not as straightforward as that. The person may not be allowed to freely access such assets, or may not have the key to perform the recovery process.

From the DRP perspective, cryptographic facilities, such as key management centres and Certification Authorities (CA), must also be brought back on-line following a disruption. Ensuring that keys remains secure while they are made available from back-up sites is just one of the complicating factors. Split knowledge in the form of a secret sharing scheme or dual control can be utilised. However, the back-up site for a certificate authority should use a separate certificate root since the integrity of the signature system is derived from the non-disclosure of the root key which is outside of the certificate authority’s key generation device.

If, for example, an organisation uses cryptographic facilities to secure its communication, it must be ensured that those facilities (e.g. CAs, key management server) operate with the same security after a disaster.

Need for crypto DRP

Therefore every organisation must have a DRP for its crypto facilities. The crypto DRP can be complicated because one simply cannot run a back-up for a CA key service as in the case of a 'normal' database. Due to the confidential character of the data, there must be a secured back-up that has to be restored in a secure way by trusted staff.

3.11.4.2 Cryptographic Disasters

Dealing with cryptographic disasters

Clear instruction to recover from cryptographic failure

The second relationship between a DRP and cryptography is planning how to deal with events caused or made complicated by cryptographic services, especially unforeseen failures. As an example, an institution may have an up-until-now-secure logical access control system, yet has noticed clear signs of an intruder into the system. One possibility is that the cryptographic system has failed. In such a situation, there should be clear instructions on how to proceed. Without such instructions, well-intentioned acts may exacerbate the problem. For example, attempting to unravel cipher text by modifying it may cause permanent damage.

Key escrow may help in emergency situations

Another example of a cryptographic disaster is the encryption of vital information by an employee who is now demanding a ransom for the decryption key in exchange for a gain. Such a problem may be solved through technical means (escrow), law enforcement, or negotiation. Unless the organisation plans for a technical solution, other solutions may be expensive, embarrassing, or both.

No complete list of threats exists and a complete list of counter-measures is impossible to produce. As a general guideline on this issue of cryptographic disaster, an information and communications security and disaster recovery programmes of an organisation must address cryptographic threats, at least in a generic form.

A written policy should cover the following:

(a) regular monitoring of the information processing system for abnormal behaviour;

(b) procedures to be followed in determining the cause of abnormal behaviour and guidelines on how to respond to a threat, intruder, compromise, etc;

(c) procedures for dealing with the failure of any cryptographic control; and

(d) provision for the availability of cryptographic services, keying material, and other related services following business interruption.

3.11.4.3 What to do in the Event of a Cryptographic Disaster

Take steps according to the incident reporting mechanism when crypto disaster occurs

Following a disaster, the officer responsible for ICT security in a department is required to act based on the *Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)* as per Appendix H.

3.12 Public Key Infrastructure (PKI)

What is a PKI?

An 'infrastructure' is a set of facilities which enable and promote certain types of activities. A set of public infrastructure such as roads, bridges, and airports facilitates transportation for economic activities. A Public Key Infrastructure (PKI) is the combination of software, encryption technologies, and services that enables organisations to protect the security of their communications and business transactions on the Internet.

More secure method is digital signature

Nowadays, apart from password-based logons, a more secure method is to use digital certificates. Each certificate contains specific identifying information about a user, including his name, public key and a unique digital signature, which binds the user to the certificate. Certainly, certificates should not last forever. Each certificate is issued with an expiry date and sometimes will need to be revoked early, such as when an employee quits. As with key pairs, there is a need to co-ordinate the issuance and revocation of certificates. That is another function of a PKI, acting as a comprehensive architecture encompassing key management, the registration authority, certificate authority and various administrative tool sets.

A PKI integrates digital certificates, public-key cryptography, and certificate authorities into a total, enterprise-wide secure network architecture. A typical enterprise's PKI includes issuance of digital certificates to individual users and servers; end-user enrolment software; integration with organisational certificate directories; tools for managing, renewing, and revoking certificates; and related services and support.

PKI protects information assets in several ways:

(a) Authenticate Identity
Digital certificates issued as part of a PKI allow individual users, organisations, and web site operators to validate the identity of each other.

(b) Verify Integrity
A digital certificate ensures that the message or document the certificate 'signs' has not been changed or corrupted.

(c) Ensure Privacy
Digital certificates protect information from interception during transmission.

(d) Support for non-repudiation
A digital certificate validates user identity, making it nearly impossible to later repudiate a digitally 'signed' transaction, such as a purchase made on a web site.

Some services need PKI immediately e.g. e-mail, fail transfer, remote access

In the public sector, some services stand out as immediate candidates for the need of a PKI: e-mail, secure file transfer, document management services, remote access, e-commerce and Web-based transaction services. Support for non-repudiation, which ensures that transactions cannot be disowned, is also required and supplied through the use of digital signatures. Then there are wireless networks and virtual private networks, in which encryption is essential as a guarantee of confidentiality. For the corporate network and e-commerce, a single point sign-on is a common requirement.

PKI software comes in different flavours depending on whether an organisation self-develops it or procures it commercially. In each case, the certificates issued need to conform to the international standard (CCITT X.509v3 is currently the referred standard) so that interoperability to other certification authorities even overseas is ensured. It is also worth noting that until today, there still exist some doubts among industry experts on the full-fledged implementation of an internationally standardised PKI.

3.13 Trusted Third Parties (TTP)

TTP provides the vehicle for safe transactions

The market has recognised the need for enhanced security services provided by an entity mutually trusted by other entities. These services range from increasing trust or business confidence in specific transactions to provision of recovery of information for which encryption keys are not otherwise available to authorised entities. Trusted Third Parties (TTP) is the vehicle for the delivery of such services.

A TTP delivers assurances between its sub-divisions as well as between itself and external parties. An institution may choose to set up an internal TTP or subscribe to an external provider for TTP services.

3.13.1 Assurance

Criteria to be met to provide quality service

A TTP, whether internal or external to an organisation can only add value when users of the services are assured of its quality. In achieving this, a TTP must satisfy itself that the following issues are addressed:

(a) Trust
The TTP must be organised, controlled and regulated in such a way that its operation can be relied upon, checked and verified.

(b) Accredited
The TTP must be at least accredited by a recognised national or international party.

(c) Compliance
The TTP must be operated in compliance with accepted industry standards and relevant regulations.

(d) Contract
There must be a legally binding contract in place covering the provision of service and addressing all the issues in this list. There must be contracts with co-operating TTPs which also address these concerns.

(e) Liable
There must be a clear understanding as to issues of liability. Areas of concern include circumstances under which TTP may be liable for damages and whether the TTP have sufficient resources or insurance to meet its potential liabilities.

(f) Policy Statement
The TTP must have a security policy covering technical, administrative, and organisational requirements.

(g) Audit
TTP auditors must be appointed by the TTP controller.

3.13.2 Services of a TTP

The services, which a TTP provides, may include:

(a) key management for symmetric cryptosystems;

(b) key management for asymmetric cryptosystems;

(c) key recovery;

(d) authentication and identification;

(e) access control;

(f) non-repudiation; and

(g) revocation.

What is a key recovery?

Key recovery is the ability of a TTP to recover, either mathematically, through secure storage, or other procedures, the proper cryptographic key used for the encryption of information. This function would assure an institution that it can always have access to information within its information processing resources. Such a recovery service may be essential in disaster recovery. It may also satisfy law enforcement regulations for an institution to be able to produce such a key or encrypted information in answer to a lawful court order.

3.13.3 Legal Issues

Government's contract with a TTP needs to address legal issues

Government departments have higher-level requirements for record retrieval. The contract with a TTP should address specific issues relating to maintenance of keys used for encryption, authentication, and digital signature as these may need to be reproduced many years later.

Liability for the poor services of a TTP may include direct and consequential damages and must also be fully understood by the management. In the first place, the TTP must have adequate financial reserves or insurance to meet any liability.

Chapter 4 TECHNICAL OPERATIONS

This chapter discusses the management and the use of safeguards incorporated in ICT assets and other related devices. This chapter seek to explain in more detail the various option available that could be use to further enhance the management of ICT security. It covers the various aspects of computer systems, operating systems, application systems and network systems.

4.1 Computer Systems

ICT assets component

As defined in the Public Sector ICT Security Policy Framework, the ICT asset component comprises of information processing facilities such as mainframes, minicomputers, microcomputers, laptops, notebooks, palmtops, servers, workstations, departmental, corporate and personal computers as well as communication facilities and network equipment such as the facsimile, fixed line telephones, mobile telephone systems, power supplies, environmental control units, routers, bridges, switches, computer and communication hardware and software, utility programs, operating systems, documentation and applications software. The housing facility is also part and parcel of the public sector ICT asset. With regard to the ICT security of these systems and sub-systems, the following controls need to be exercised:

4.1.1 Change Control

Change control procedure should exist for hardware, software, manual procedure and emergency changes

Change Control can be defined as the processes initiated to manage and control planned changes about to occur and that the changes will affect ICT operations or its environment. The triggering Change Control events may be scheduled or in response to an emergency. ICT being volatile, Change Control is necessary to protect the integrity of information processing systems and should exist to meet changes in hardware configuration, software changes, manual procedure changes or other changes that will affect service delivery.

Establish effective change control procedure

Change control is established to ensure smooth migration and minimal operational disturbance. As such, it should be well thought off and effective. Change control should consist of at least the followings:

(a) formal change request;

(b) formal authorisation process;

(c) test and system acceptance procedure for every change to consist at least unit test, component test and integration test;

(d) fully documented changes and expected outcome;

(e) virus checks before and after changes are made, where appropriate;

(f) back-up and restore procedures to capture the system image prior to the new environment; and

(g) explanatory exercise for user buy-in.

4.1.2 Equipment Maintenance

Equipment under maintenance or scheduled for maintenance can be a vulnerability source. To ensure the integrity of equipment, implement the following security controls:

(a) ensure correct equipment is sent for maintenance and that maintenance is due or necessary;

(b) maintenance conducted by authorized personnel;

(c) remove sensitive information if possible;

(d) equipment containing sensitive information when under maintenance should be supervised;

(e) inspect and test equipment before and after maintenance;

(f) record all faults and detail of repairs; and

(g) virus checks before and after maintenance, where appropriate.

4.1.3 Disposal of Equipment

To prevent inadvertent disclosure through disposal of equipment conduct the following:

Ensure sensitive information in equipment to be disposed is properly erased

(a) erase or destroy all information regardless of sensitivity and perform confirmation. In some instances, it may be necessary to destroy the equipment; and

(b) record all disposal and method used to erase or destroy the information.

4.2 Operating systems

Secure operating systems tested against security standard such as TCSEC

There are various categories of operating systems. The most secure operating system tends to be very close and proprietary and the least secure are more open and known to many. The security level of operating systems is categorised based on well-known security standard such as the Trusted Computer Security Evaluation Criteria (TCSEC) also known as ‘The Orange Book’ and the Common Criteria (CC).

Rahsia and *Rahsia* Besar should reside on trusted OS equivalent to a B1 security level or above

It is advisable that all government computers handling *Rahsia* and *Rahsia Besar* information use trusted operating systems certified to a level equivalent to or above B1 Security of TCSEC.

Only authorised system administrator should be allowed to access host OS

Due to the fact that the operating system controls all applications running on the computer and most technical staff is capable of manipulating the operating controls, it is therefore prudent to prevent intentional or inadvertent security breaches through the operating system. If possible, all changes to the operating system should acquire prior approval and later be monitored by knowledgeable security and audit personnel. An essential rule is to disallow technical staff other than authorised system administrators to operate a mainframe, minicomputer, desktop server or have access to its operating system. Where this is not feasible, close supervision is imperative.

4.2.1 Proprietary Issues

Need to balance between security and openness

ICT Managers and planners should have in-depth knowledge and understanding of the implication of choosing specific operating systems and their impact on the legacy and future systems. As much as possible, the public sector should remain with the non-proprietary operating system to eliminate the unnecessary cost of maintenance except in instances where high security is needed.

The right balance between security and openness must be properly defined by the assistance of security specialists and to take into consideration the business needs against serious implications.

4.2.2 Shareware and Freeware Operating System Issues

The use of shareware and freeware operating system should be carefully considered. Any downloaded shareware or freeware may contain malicious code that pose a threat to the security system of the organisation.

Downloaded shareware or freeware should not be used to process government data because this may cause spreading of malicious code. If unavoidable the shareware or freeware must be screened against such code before being installed.

4.2.3 Logical Access Control

Access control is essential to prevent unauthorised access and provide fast access failure reporting

This is a set of controls employed at ICT installations aimed at permitting only authorised access and providing fast access failure reporting. Some of the access control mechanisms employed is described below:

The materials can be used to formulate departmental access control policy. The ICTSO has to decide which is mandatory, optional or conditional.

4.2.3.1 Identification of Users

Steps to ensure only legitimate users use the system

Users of ICT systems can be an individual or a group of users sharing the same grouped user account. In both circumstances, users should assume responsibility for the security of the ICT system they are using. Some of the steps undertaken to positively identify legitimate users of the ICT system are:

(a) assign a unique user ID to each individual user. It is best to consult the user on the actual ID to be used rather than assigning a pre-determined user ID. In other words allow the flexibility for the user to choose his or her own ID or provide the ability to change the ID on first use;

(b) hold each and every individual accountable for all activities under the registered user ID;

(c) ensure that there are auditing facilities to trace all user activities; and

(d) ascertain that all user IDs are created upon legitimate departmental request and leave no opportunity to create unneeded user IDs.

In ensuring that unused user IDs (example due to long leave, attending courses, etc) are not misused:

(a) suspend all user privileges after 30 days of non-use and delete after 30 days suspension; and

(b) revoke immediately all privileges of users who have been re-assigned, transferred or terminated.

The system administrator should be informed on occasions where users are away from the office for a duration of more than seven (7) days so as to enable periodic monitoring.

It is good practice to archive audit trails of user activities

It is possible that security incursions might have occurred in the past without being detected. Therefore it is good practice to archive audit trails of user activities. However, the down side of such activity is storage requirement. It is recommended that activities of users who have access to sensitive information be archived.

4.2.3.2 Authentication of Users

Authentication is normally by passwords

One of the salient principles of ICT security is the authentication process that confirms the validity of the user or point of origin of the communication through the use of passwords. It is further strengthened by controls such as the requirement for all users to make immediate reports in cases of lost, compromised, suspected loss or suspected compromised passwords.

In order to minimise password disclosure:

(a) passwords should be entered in a non-display field;

(b) be of minimum length of eight (8) characters;

(c) require and enforce that passwords be changed at least once in 30 days;

(d) make available distress passwords for sensitive operations (a distress password is different from the normal user password and is used as a pre-arranged signal to indicate duress or coercion);

(e) passwords shall not be shared or made known to others, including administrators;

(f) instruct users not to use easily guessed passwords, i.e., own names, phone numbers, date of births, common words or numbers;

(g) use combinations of both alphabets and numeric characters;

(h) all passwords should be memorised and be stored in a secured location if required to be written down;

(i) encrypt password during transmission, where possible;

(j) store password files separately from the main system application data;

(k) prevent reuse of the user’s last four (4) passwords;

(l) prohibit the display of passwords on input, reports, or other media; and

(m) one time password - the generation of new passwords for each session using pre-determined information that the user possesses or knows.

Proper authentication through use of dynamic passwords can be assured by implementing some of the following measures:

(a) selecting authentication tokens that are user changeable or activated by biometrics data;

(b) prohibiting the sharing of token PINs;

(c) ensuring that security tokens are resistant to tampering and duplication;

(d) using a different PIN from the user ID;

(e) using the PIN of minimum eight (8) length characters;

(f) randomly generated passwords to be used only once;

(g) encrypting keys and other information critical to authentication within the token and on the validating system;

(h) locking access after three (3) invalid tries;

(i) maintaining an inventory control on security tokens;

(j) requiring employees to acknowledge receipt of security tokens and explain conditions of use together with consequences of misuse;

(k) taking steps to recover immediately dynamic tokens from the employee upon reassignment or termination and terminate access privileges associated with the token assigned to the employee;

(l) conducting one-time challenge i.e. the ICT system challenges the authentication of the user when users log-on. To provide the answer, a specialised (hand-held) device would normally be used where upon input of the challenge, the authentication code is revealed. The user then proceeds to submit the authentication code. The authentication code is only used once and not repeated;

(m) using the digital certificate and electronic signature i.e. the use of a trusted third party appointed by the government; and

(n) using Biometrics or the process of using a unique attribute held by the person as a means of identifying that person including fingerprints, iris patterns, voice, face geometry, the shape and size of hands and fingers etc.

4.2.3.3 Limiting Log-on Attempts

Maximum logging attempts limited to 3

It is recommended that log-on be limited to three (3) attempts. The user ID should be suspended after the maximum of three consecutive unsuccessful log-on attempts. To begin investigation of attempted log-on, use the information detailing the attempted log-on as a reference point. The legitimate user should also be informed of such attempts.

Where authentication is used, there should be a time limit to verify the authentication. It is suggested that the authentication time limit be set to two (2) minutes (depending on organisation or location of logging-on) upon which the session is terminated.

4.2.3.4 Unattended Terminals

Ensure safety procedures are carried out on unattended terminals

In order to prevent unauthorised use of unattended terminals connected live to a system:

(a) activate the authentication process after a 10 minutes lapse of inactivity before allowing work to continue;

(b) activate a one-button lockup or initiate shut-down sequence when terminal is inactive;

(c) avoid storing passwords or any information that can be used to gain access on workstations; and

(d) implement password screen saver.

4.2.3.5 Warning Messages

Display warning against unauthorised access clearly

It is recommended that all users be reminded of their accountability when accessing ICT resources. This could be done, prior to log-on, by displaying a warning against unauthorised access or improper use and the consequences for such activity.

4.2.4 Audit Trails

Audit trails are records useful in events of mishaps

Audit trails are records of activities used to provide a means of restructuring events and establishing accountability. The audit trail information is essential in an investigation when problems occur.

Provide an audit trail for computer systems and manual operations when:

(a) critical information is accessed;

(b) network services are accessed; and

(c) special privileges or authorities are used, such as, security administration commands, emergency user IDs, supervisory functions, and overrides of normal processing flow.

Include in the audit trail as much of the following as is practical:

(a) user identification;

(b) functions, resources, and information used or changed;

(c) date and time stamp;

(d) workstation address and network connectivity path; and

(e) specific transaction or programme executed.

Provide additional alarm for security related events

Provide, where practical, an additional real-time alarm for significant security-related events such as:

(a) access attempts that violate the access control rules;

(b) attempts to access functions or information not authorised;

(c) concurrent log-on attempts; and

(d) security profile changes.

In such cases:

(a) investigate and report suspicious activity immediately;

(b) ensure that System Administrator reviews the audit trail information on a timely basis, usually daily;

(c) investigate and report security exceptions and unusual occurrences;

(d) retain the audit trail information for an appropriate period of time for business requirements; and

(e) protect audit trail information from deletion, modification, fabrication or re-sequencing, by use of Machine Access Control (MAC) or digital signature.

4.2.5 Back-up

In order to ensure that the system can be recovered in the event of a disaster, regular back-up should also be done whenever the configuration of an operating system is changed. This back-up must be kept in a secure environment.

When doing back-up, consider:

(a) document back-up/restore procedures;

(b) keeping three (3) generation of back-ups;

(c) keep back-up copies off site; and

(d) test back-up media and restore procedures.

4.2.6 Maintenance

In order to maintain, the integrity of the operating system against security breaches and vulnerabilities, employ the following controls:

4.2.6.1 Patches and Vulnerabilities

New vulnerabilities and bugs are constantly being discovered and once discovered they are broadcast and released by authorised security agencies such as Malaysian Computer Emergency Response Team (MyCERT), Canadian Computer Emergency Response Team (CCERT) or Australian Computer Emergency Response Team (AusCERT) as well as software providers like Microsoft. It is the role of the ICTSO or System Administrator to be aware and keep abreast of this development issued by Government Computer Emergency Response Team (GCERT) and implement the suggestions.

4.2.6.2 Upgrades

Procedures should be established to maintain the most current version of the operating system. However the decision to upgrade to the latest version need to be evaluated based on its implication to the overall system operation as well as cost incurred.

4.3 Application System

Public sector uses both commercial and internally developed software

Within the public sector a mixture of commercially and internally developed application software have been installed and are in use. In general, all access to software must always be justified and authorised.

The following controls should be implemented for the protection of software and the information that it processes:

4.3.1 Application Software

Implement ICT security control within applications

Within the application of the software, ICT security control should be implemented to prevent unauthorised access, modification, disclosure, or destruction of information. Some of the controls include:

(a) an integrated system security with an operating system access control facility, that allows for centralised and standardised user ID and password management;

(b) an established access profile structure that controls access to information and functions based on need-to-access requirement;

(c) consistent access controls on information that is replicated on multiple platforms. For example if a person is allowed to have read access to information in a certain operating system (e.g. Windows), this read access right applies to the other operating system (e.g. UNIX);

(d) an application control that identifies specific accountability of a user using a user ID. All transaction details should at least be logged with a user ID, showing time, date and activity;

(e) an information ownership incorporated system, where ownership may be accountability on a group or individual level;

(f) an application of the location control method that restricts access at specified locations or areas;

(g) dual control capabilities for identified critical transactions. Example: the requirement to have two (2) persons holding a user ID and password to transact monetary movement; and

(h) immediate logging and report of violation messages in case of occurance.

4.3.2 Databases

Databases need to be protected from unauthorised access

Controls should be implemented to protect databases from unauthorised modification or destruction. The integrity of information stored in databases can be maintained through the following:

(a) a database management system that ensures the integrity of updating and retrieval of information. Concurrent control is required for user-shared databases;

(b) a controlled access to information specified by either System Administrator, ICTSO or CIO; and

(c) an access control mechanism to physical information resources to restrict access to authorised information management systems, applications and users.

4.3.3 Systems which Employ Artificial Intelligence

Security controls should be included in AI based application system

Applications using artificial intelligent (AI) techniques such as automatic decision-making should include controls specific to that technology as follows:

(a) secure knowledge bases used by inference engines or similar AI processing techniques as well as a regular review for accuracy and effectiveness;

(b) set a maximum limit on automatic decision making ability of AI systems or AI sub-systems of conventional applications to ensure that unexpected errors of failures can be determined;

(c) an AI system which is used to make highly sensitive decision must not be set in a totally automated mode. Instead it should act in an interactive mode with humans to ensure that vital decisions are approved;

(d) set controls on information used in training of neural networks based applications;

(e) monitor the stability of neural network based-applications for effectiveness; and

(f) build all AI systems within programmed decision enclosures to ensure that the control of decision-making is kept within reasonable limits according to the information being processed.

4.3.4 Application Testing

Testing to ensure applications function according to specifications

One aspect of application systems development using the Software Development Life Cycle (SDLC) methodology is that of testing, which is required during the final stage of development. It involves the testing of a newly acquired application, upgrading an application or migration from old to new hardware. This is required to ensure that systems are working according to specifications.

Protect data during testing

In order to protect information from disclosure or inappropriate processing during application testing:

(a) use dummy or historical data for testing purposes;

(b) establish a policy that controls the use of classified information during application testing and use access control to limit access to appropriate personnel only;

(c) dispose of information used in the system during testing (especially when using the historical data); and

(d) require the use of physically separate environments for operational and development systems. This can be applied by establishing a development environment for the developers to design, develop, test and integrate the application systems.

4.3.5 Defective and Malicious Software

Internally developed or outsourced software could be defective

Development of software can be categorised into two (2) types: internal development or outsourcing. Both cases will encounter the defective software. In most cases the defect will be determined during the testing stage.

However, to minimise the probability of latent defects in software, controls should be properly implemented as follows:

(a) require the software acquisition system to select vendors with a good reputation, a proven record and sufficient resources. This is an important criterion to minimise the possibility of the supply of defective software. It will also improve the level of confidence in the acquisition of the software;

(b) establish a quality assurance programme and the procedure for all software developed internally or acquired externally;

(c) require that all software be fully documented, tested and verified to its maturity, robustness and effectiveness; and

(d) if it is discovered in the future that the software provider has inadvertently included malicious code into the software system (e.g. system may be used for international espionage or intelligence gathering on government information) then a liability clause must be included in the contract.

Users are required to report defective or malicious software to the helpdesk.

4.3.6 Change of Versions

Control and maintain integrity of software with new versions and upgrades

Software (application, OS, utilities, tools) is upgraded regularly. New versions are issued to ensure it is bug free and to upgrade functionalities. However changing of software versions should be controlled to maintain the integrity of the software when changes are made and this requires change control procedures to be followed [Refer to 4.1.1 Change Control].

4.3.7 Availability of Source Code

Consider escrow agreement for purchased software for which source code is not available

If the software system were developed internally, the source code would be easily available. However, if the system is purchased off the shelf, most vendors do not supply the source code to their customers. In order to ensure that source code is available for debugging or enhancement, controls should include the following:

(a) establish procedures to maintain the most current version of programmes written; and

(b) consider an escrow agreement for purchased software for which source code is not available in the event of disaster or national security breach.

4.3.8 Unlicensed Software

Unlicensed software is illegal

Unlicensed software is illegal. The Malaysian Copyright (Amendment) Act 1997 specifically prohibits the use of unlicensed software. The Ministry of Domestic Trade and Consumer Affairs enforces this Act and monitors the use of unlicensed software.

Usage of licensed software means software for which a license has been issued and control of inventory such as the safe keeping of the license. The inventory includes the physical control of the location of the licensed software and a copy of the license issued.

4.3.9 Intellectual Property Rights

IP rights for developed software should be specified in the contract

The Intellectual Property (IP) right is the right to claim ownership of a document, software or other creation.

Commercial software products are usually supplied under a license agreement that limits the use of the products to specified machines and may limit copying to the creation of back-up copies only.

In order to prevent infringement of intellectual copyrights due to unauthorised copying of software on mass storage media, compliance to the Malaysian Copyright (Amendment) Act 1997 must be ensured at all times.

It is recommended that the IP rights for in-house or jointly developed software be specified in the contract.

4.3.10 Malicious Code

In order to maintain the integrity of information and protect it from disclosure or destruction from malicious code such as viruses, Trojans or worms, the following controls should be applied:

(a) install a system and implement a procedure to manage malicious code. All software acquired should be screened for such code prior to installation and use;

(b) establish a written policy on downloading, acceptance and use of freeware and shareware;

(c) authenticate software for applications using MAC or digital signature. Failure to verify indicates a potential problem and all use of the software should be halted;

(d) distribute instructions on the detection of malicious code to all users;

(e) establish a policy and procedure for the checking of diskettes; and

(f) seek assistance in case of suspected infection. Assistance may be sought from internal technical staff and/or vendors.

In ensuring recovery of processing capability following a malicious code attack, certain steps need to be performed including the following:

(a) retain an original back-up copy of all software, data and information for the purpose of restoration; and

(b) ensure that all data are backed up regularly.

In the case of virus infection, the following steps are recommended:

(a) use the approved virus application software;

(b) scan the virus using the facility from the software;

(c) delete and/or remove the virus immediately; and

(d) check the status of the scanning from the software report log.

4.3.11 Unauthorised Memory Resident Programs

Perform periodic inspection of installed software

Memory Resident Program (MRP) is a program that is loaded into memory where it remains after it finishes its task, until it is explicitly removed or until the computer is turned off or reset. The program can be invoked again and again by the users (with the aid of a hot key) or by an application. In order to prevent unauthorised MRP, for example those that allow seemingly normal processing to take place but retain ultimate control over functions of the processing resource, perform periodic inspection of software installed to ascertain whether any unauthorised software has been inserted:

(a) implement additional controls (based on business needs) such as, token-based authentication devices, security modems that can provide password and dial-back controls or remote computing software that can provide password controls; and

(b) use secure remote access approved equipment.

4.3.12 Software Provided to External Parties

Secure a dedicated environment for software or insist on written statement from vendors

There may be cases where software is provided by government to external parties such as a private company owned by the government. In order to prevent unauthorised destruction or modification of such software, the following controls should be implemented:

(a) create and secure a dedicated environment for diskettes, CDs or other storage media. This should include physical and logical controls on the hardware, software and diskettes used for creation, copying, and protection; and

(b) require a written statement from distributors of software against malicious code.

In order to protect the public sector against claims of negligence due to the use of provided software, ensure the following controls:

(a) execute an agreement with external parties to whom software is provided that enumerates each party’s responsibilities, required security duties and limits on liability; and

(b) maintain sufficient documentation to prove that the provided software was not the cause of viruses or other malicious code.

4.3.13 Software from External Sources

Prevent introduction of unauthorised software from external sources into the system

Care should be taken to prevent software being introduced into the domain through software downloading facility without the specific request or consent of the department. As an example, software providers will often download software to their customers. Another example is the downloading facility set up by vendors to distribute the latest version of the software.

In order to prevent unauthorised software from appearing in the system include the following:

(a) establish procedures on the downloading of software from external sources;

(b) organise a mechanism where downloaded software can be distributed into a server in a demilitarised zone (DMZ) to be accessed by a System Administrator later; and

(c) require the firewall to include virus scanning or ensure that any executable file is scanned for viruses before it is introduced into the network.

4.4 Network System

Measures to protect network equipment

A network is a system, which interconnects a multitude of computers and workstations for the purpose of communications and information/resource sharing. In keeping the various interconnected parts of the system interoperable, rules and procedures must be established. In a secure processing environment, networks have additional ‘layers’ of rules and procedures imposed, each addressing unique security requirements, with no one set of requirements (software or hardware) applicable to all security issues for any specific situation.

Problems could occur because there are layers of security, each very narrowly focused for specific conditions. In case of ever emerging systems and new equipment with greater capabilities and a multitude of abbreviations and operating names, ‘old’ rules can be easily forgotten in favour of simple ways of dealing with security, regardless of the layers involved. This tendency has created both the need for increased understanding of the various security layers when using shared resources in multi-secure network environments, and also the need for continuing industry awareness of network security problems.

Customers or contractors being seriously interested in connecting to governmental network must have all applicable security policies, standards, and procedures, before access is granted. These requirements should ensure that minimum-security practices are always in place. Password protection for local file servers must be enforced for all users before access to the network is granted. Local hosts must report all non-local site accesses. This auditing capability should ensure unauthorised accesses are traceable.

4.4.1 Securing a Network

Add-on controls

Poor administrative practices and the lack of education, tools, and controls combine to leave the average system vulnerable to attack. Research promises to alleviate the inadequate supply of tools and applicable controls. These controls, however, tend to be add-on controls. There is a need for the delivery of secure complete systems, rather than the ability to build one from parts. The average administrator has little inclination to perform these modifications and no idea how to perform them.

Extensive connectivity increases system access for hackers. Until standards become widely used, network security will continue to be handled on a system-by-system basis. The problem can be expected to increase if and when the Integrated Systems Digital Network (ISDN) is implemented without appropriate security capabilities.

A promising note for the future does exist. Multiple sets of tools do not need to be developed in order to solve each of the potential threats to a system. Many of the controls that will stop one type of attack on a system will be beneficial against many other forms of attack. The challenge is to determine what is the minimum set of controls necessary to protect a system with an acceptable degree of assurance.

4.4.1.1 Design of a Secure Network

Ensuring end-to-end security for a secure network

The design of a secure network shall consist of network elements that cater for end-to-end security. The design must first undergo a process of security assessment during which the organisation states its aims and objectives, scope of security and whether there is a need for end-to-end security, inter-network security or security at the internal systems only. From here the organisation then combines the business needs and network risk analysis.

The next step is to identify and determine the assets that need to be protected, including the information types, where and the degree/level of security protection needed. After all assets and their security requirements are determined, the network and systems architecture to support the different objectives and aims has to be established, taking into account the security needs of each system and application.

The design must also identify potential threats and vulnerabilities, and establish the preventive systems, policies and procedures to protect the information. The finished design can take many forms but for the purpose of these guidelines, a generic architecture is described as in the figure below:

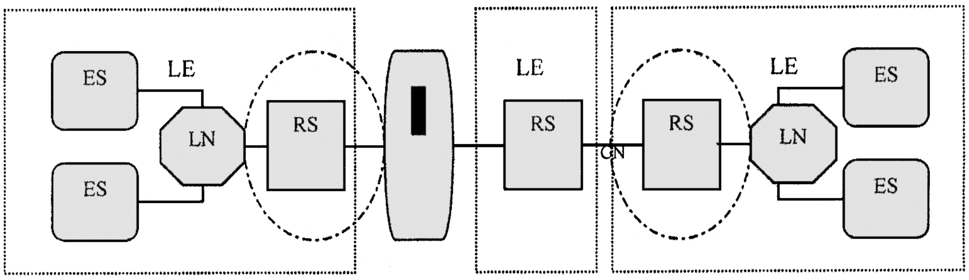


Figure 4.1: Generic Network Security Architecture

Key :

ES = End System	RS = Relay System
LN = Local Network	LE = Local Environment

From Figure 4.1 above, the generic network security architecture applies to any network-to-network connectivity. The most vulnerable part of the network is RS where the router and switches are located. It is at this point of the network that security gateways are normally placed in the form of firewalls or other security equipment that cater for data encryption, data origin authentication, data integrity and access control. All these must also be included based on the requirements identified during the security assessment process.

The security gateways can be a simple firewall that separates connections to other networks and the two network zones; namely the DMZ and the secure zone. It may also include VPN modules and/or encryptors/decryptors.

The other considerations at the department’s client premise include the need to have Intrusion Detection System (IDS), virus scanners and data encryption at the local environment (LE). The decision to use IDS is also subject to requirements that are determined during security assessment.

4.4.1.2 Network Security Controls

Ensuring a range of appropriate security controls

Appropriate controls should be established to ensure security of data in private and public networks, and the protection of connected services from unauthorised access.

A range of security controls is required in computer networks. Individual users should be aware that connecting their computer to the network could allow unauthorised access to private data if appropriate controls are not established. Documentation should be available to the user detailing how to adequately secure their data should they wish to make it available on a network.

Network managers should ensure that appropriate controls are established to ensure the security of data in networks, and the protection of connected services from unauthorised access. Special attention is required to protect sensitive data passing over public networks like the Internet.

4.4.2 Security of Network Equipment

In order to effectively include security in the procurement process of network systems or equipment, it must be integrated into the procurement cycle from its inception. Sufficient information about the procurement cycle is included to allow a person not familiar with the procurement process to understand the need for incorporating computer security into the procurement cycle.

Acquisition planning can only begin after an agency has determined that a need exists. The need determination phase is very high-level in terms of functionality. No specifics of a system are defined here. The idea for a new or substantially upgraded system and the feasibility of the idea need to be explored. During this early phase of the acquisition, the definition of the security requirement should begin with the preliminary sensitivity assessment.

The preliminary sensitivity assessment should result in a brief qualitative description of the basic security needs of the system. These should be expressed in terms of the need for integrity, availability, and confidentiality. This does not require an elaborate sensitivity analysis scheme, but must include an assessment of the significance of the systems. Legal implications, federal policy, agency policy, and the functional needs of the system help determine the sensitivity of a system. Factors including the importance of the system to the agency mission and the consequences of unauthorised modification, unauthorised disclosure or unavailability of the system or data should be considered when assessing sensitivity.

4.4.2.1 Installation Security

Pre-installation security check

After undergoing a security check during the procurement process, any equipment that is to be installed must have undergone a Factory Acceptance Check (FAC), prior to installation, and then configured.

4.4.2.2 Physical Security

Ensuring physical security

The following standards of physical security must be observed:

(a) premises housing network control equipment must be physically strong and free from unacceptable risk such as flooding, vibration, dust, etc;

(b) air temperature and humidity must be controlled to within equipment defined limits; and

(c) network electronics must be powered via Uninterruptible Power Supply (UPS) to provide the following:

i. minimum of 15 minutes' operation in the event of a power blackout; and

ii. adequate protection from surges and sags.

4.4.2.3 Physical Access

(a) Network Cabling Access

Protection against unauthorised access

As far as practical, network infrastructure must be protected from unauthorised access. Tools are readily available which allow network ports to be monitored, or the operation of the network to be disrupted. In order to minimise the risk of network interference consideration should be given to:

i. protecting cabling in public areas with conduits or other protective mechanisms;

ii. in a structured wiring area, ensure that network and telephone points that are not in use have been detached from the active network or telephony equipment;

iii. telephony and networking risers and data cabinets can only be accessed by authorised personnel;

iv. information, which is being transferred over a less secure network (e.g. the Internet) is encrypted; and

v. highly accessible access points such as networked modems should have associated and appropriate security mechanisms.

(b) Network Equipment Access

All network equipment should be placed in physically secure areas. This includes, but is not limited to, backbone and access routers, hubs, bridges, and gateways. Network file servers are covered by this policy as well, especially when acting as a router between LAN types, such as Ethernet to Token Ring. Networking equipment should not be placed in an office environment. Rather, such equipment should be placed in the communications room of the office building being served, and access restricted to authorised personnel. In addition:

i. access to areas housing network electronics shall be controlled by designated ICTSO; and

ii. doors to areas housing network electronics should be locked with a unique key, the distribution of which will be determined by the ICTSO.

4.4.2.4 Logical Access

(a) An ID and password should be required to gain access to router software. Only authorised personnel should be provided access, along with the minimal privileges required for performing the necessary tasks. The ICTSO administers the creation of the router IDs, passwords and privileges. Proper management authorisation should be required for all access requests. A list of these ‘management authorisers’ must be maintained and updated at least once a year. Requests for access must be maintained for the life of the IDs.

(b) Password composition and maintenance must be consistent with the guidelines. Passwords must be changed approximately every 30 days, as well as after security events, in emergency situations, when an employee transfers, or any other incident in which the password may be compromised.

(c) All access to routers must be logged and maintained, including the person, time of day, and nature of activity. This information must be maintained for 90 days. Daily audit trails are to be monitored for unauthorised access attempts. Managers will take appropriate action with respect to all unauthorised access attempts.

(d) The network should only accept traffic from properly registered addresses. All router software changes must be logged, including the person making the change, management approval of the change, date and time. Access via modem will be accommodated only under strictly controlled conditions.

(e) Router configuration change authority is to be centrally managed. All routers should have active filter tables to ensure that only authorised access is allowed. In environments where information is especially sensitive, additional precautions may be required, such as data encryption, and security gateways. These precautions should be taken as requested or required, and will be offered as additional service to the base level.

4.4.2.5 Unauthorised Use of Equipment

Controlling unauthorised use of equipment

The unauthorised use or interruption of network equipment can be prevented by:

(a) controlling access to network equipment by logical access controls listed above;

(b) locating network equipment in a physically secure environment;

(c) erecting a physically secure wiring closet, accessible only by authorised personnel;

(d) routing network cabling underground or through conduits, wherever possible;

(e) maintaining an inventory of network equipment, which is periodically reviewed; and

(f) prohibiting the use of any unauthorised modem.

4.4.2.6 Equipment Configuration

Ensure correct configuration of equipment

On critical network subnets, it is absolutely important to correctly configure network equipment. It is imperative to check for the following:

(a) enable only needed services;

(b) restrict access to configuration services by port/interface/IP address;

(c) disable broadcasts;

(d) choose strong (non default) passwords;

(e) enable activity logging; and

(f) carefully decide who should have user/enable/administration access.

4.4.2.7 Equipment Maintenance

Proper maintenance of equipment

Equipment should be installed, operated and maintained according to the manufacturer’s specifications. Properly qualified personnel should carry out maintenance.

Equipment should:

(a) be installed and operated within the manufacturer's specifications;

(b) be maintained in accordance with the manufacturer's recommended service intervals and specifications;

(c) be repaired and serviced only by properly trained and authorised service personnel; and

(d) have a maintenance record of all faults or suspected faults. Not only does this aid the diagnosis and repair procedure, but may be used to document warranty and other claims.

Ensure that the integrity of security controls is maintained during equipment maintenance by:

(a) allowing modifications to be made only by authorised personnel within established maintenance procedures;

(b) insisting on testing of controls, both before and after maintenance changes;

(c) maintaining a record of all faults or suspected faults;

(d) ensuring virus checks are made where appropriate; and

(e) tamper-protecting components which store sensitive information.

4.4.2.8 Disposal of Equipment

Proper disposal of equipment to prevent disclosure of sensitive information

In order to prevent disclosure of sensitive information through disposal of equipment conduct the following:

(a) check all equipment containing storage media for sensitive information prior to disposal;

(b) perform a risk assessment on damaged equipment to determine if it should be destroyed, repaired or discarded; and

(c) ensure storage media undergo a secure erasure procedure prior to disposal.

4.4.3 Securing Different Modes of Communications

Security threats from different modes of communications

Different modes of communications discussed in this section include wired and fixed network, wireless communications, microwave communications and satellite. These different modes pose different types of security threats and ways of prevention as discussed below.

4.4.3.1 Wired Network

A wired Network is a network that uses the conventional copper or more recently, the optical fibre as the medium of communication. Presently, the wired network is the most predominant in the networking world as can be seen in the next paragraph.

Apart from the telephone private networks, one of the fastest growing sector is the area of Local Area Network (LAN). An area that is growing at an even faster rate is the product that links multiple LANs together. Hence, today the Internet is seen as an explosion of networks inter-linking thousands and millions of LANs. Today these networks are interconnected through physical wires or cables, especially LANs. However, the availability of wireless LANs will certainly change the future network environment.

4.4.3.2 Wireless Communication

Wireless applications involve the technology of presenting and delivering wireless communication information to and from telephony terminals, other wireless terminals, within a LAN and within networks. A wireless application is utilised when a telephony terminal, e.g. mobile phone communicates with a server installed in the mobile telephony network.

Wireless LAN systems are usually made up of a cell or group of cells that contain several wireless station adapters in each of them. Each cell is controlled by an Access Point, (a device that is usually connected to an existing backbone), and which manages all the traffic within the cell. Station adapters within the coverage area of an access point (i.e. the cell) can communicate between themselves, or gain access to wired LAN resources through the access point. Station adapters associated with an access point are synchronised with it by both frequency and clock, so they can transmit and receive data to and from the access point. The same rule applies for interception - in order for someone to intercept the data one must be within the coverage area of the cell and be synchronised with the access point.

There are two types of wireless protocols that are widely used today. Direct Sequence (and also narrow band) wireless LAN systems work in a predefined constant frequency, i.e. when the user buys an access point or a station adapter it is working in a certain constant frequency. In this case it is easier to detect the frequency of the carrier wave and to synchronise with it. With Frequency Hopping systems, the frequency of the carrier wave is continuously changing. It is difficult to detect the current frequency of transmission and even if it is possible, it changes within milliseconds.

Secure wireless connection can be assured by:

(a) implementing a secure wireless protocol that will uphold data integrity, privacy, authentication and protect from denial-of-service;

(b) providing controls for the detection and reporting of dropped communications and timely termination of all associated sessions; and

(c) requiring re-authentication when wireless connection drops occur.

Eavesdropping of the wireless signalling can be prevented by:

(a) establishing a policy setting out conditions under which wireless access is permissible;

(b) implementing, where business needs dictate, additional controls such as, frequency hopping;

(c) encrypting classified information during electronic transmission; and

(d) protecting passwords by encryption.

Corruption or modification of information during transmission can be detected by authenticating information with digital signature. Establishing a procedure for safeguarding and use of wireless equipment can prevent unauthorised use or interruption of wireless equipment such as wireless network access equipment, wireless PC cards and Wireless Applications Protocol (WAP) enabled devices.

4.4.3.3 Microwave Communication

Some parts of the government network will include microwave communications systems as part of the overall infrastructure. Microwave equipment uses ‘focused’ transmission techniques between transmitting and receiving dishes. Microwave communication is basically a Frequency Modulation (FM) radio at a specific frequency and modulation. It is a point-to-point of line-of-sight communications.

A security procedure should be established to ensure secure microwave communications as follows:

(a) data encryption - a clear procedure on data/information transmission;

(b) physical access - access to communications equipment (network facilities) should be controlled and restricted;

(c) provide controls for monitoring, detecting and reporting of dropped communications due to Radio Frequency Interference (RFI), weather effects, etc; and

(d) provide control over acquisition processes by ensuring appropriate equipment is purchased.

4.4.3.4 Satellite

The primary role of a satellite is to reflect electronic signals. In the case of a telecom satellite, its primary task is to receive signals from one ground station and send them down to another ground station located a considerable distance away from the first. This relay action can be two-way, as in the case of a long distance phone call.

Another use of the satellite is when, as is the case with television broadcasts, the ground station’s uplink is then downlinked over a wide region, so that it may be received by many different customers possessing compatible equipment. Still another use for satellites is observation, wherein the satellite is equipped with cameras or various sensors, and it merely downlinks any information it picks up from its vantage point.

The advantage of satellite communications is a high degree of reliability and availability. Furthermore, satellite operator normally add back-up satellites to further enhance the already high degree of redundancy. There is also very minimum number of points where network security vulnerabilities exist (i.e. the satellite itself and the ground station). However, satellite communications normally co-exist with fixed network communications. This requires security measures and procedures to be applied according to the fixed network guidelines.

4.4.4 User Accessibility

Assigning user accessibility

As a general rule, the assignment of network access privileges and control of proxy accounts and default network accounts for all network users shall be centrally controlled, authorised and documented.

The material presented below may be used to formulate a policy on network services.

4.4.4.1 Local Area Network

Within the boundaries of the LAN, intrusion protection is required to prevent:

(a) government employees from indiscriminately plugging laptop computers into any access port of the LAN;

(b) unauthorised access of government employees to strategic systems, by ensuring that:

   i. only those computers belonging to the Government will be allowed to function when connected to the LAN. Visiting personnel wishing to access the network must have authorisation from the system administrator, who must apply to the ICTSO for temporary access rights; and

   ii. no unauthorised user should be allowed network access to strategic computing systems.

Insider attacks or unauthorised access to internal networks can be prevented by the following measures (note: most attacks come from the inside):

(a) no 'sniffer' or 'network analyser' software is to be allowed on any PC unless it has been authorised by the network manager in consultation with the ICTSO. The status of these machines should be reviewed yearly;

(b) on systems, where such software utility is standard, the software should either be deleted or permissions changed so that it can only be used by root. In this case the user must not have access to the root account; and

(c) installing a packet filter/firewall between internal networks and class systems.

Hubs, bridges and routers are getting very intelligent, with more and more configuration options and are increasingly complex. This is useful for additional features, but the added complexities increase the security risk.

4.4.4.2 Remote Access

Remote access is the capability to access information-processing resources via public or private networks. In order to ensure that remote access controls are not compromised the following need to be adhered to:

(a) establish a policy stating the conditions where remote access is permissible;

(b) implement additional controls (according to business needs) such as token-based authentication devices, security modems that can provide password and dial-back controls or remote computing software that can provide password controls;

(c) require written permission when external access is absolutely necessary. These external connections can be classified as incoming or outgoing; and

(d) use secure remote access approved equipment.

Examples of incoming connections are:

(a) dial-up access for organisation / partners;

(b) dial-up access for ICT staff and directors;

(c) access from universities (co-ordination on research projects);

(d) Internet e-mail;

(e) enterprise WWW server; and

(f) Electronic Data Interchange (EDI).

Examples of outgoing connections are:

(a) access to vendor bulletin boards (for getting information, drivers);

(b) customer connections (providing special services to public);

(c) Internet e-mail;

(d) normal Internet access: WWW e.g. Netscape/Internet Explorer via proxy server;

(e) special Internet access: e.g. Archie, ftp, news, telnet, gopher and WAIS; and

(f) EDI.

External contractors must also comply with the public sector's ICT Security Policy. In addition, the department needs to:

(a) execute a written agreement with external parties identifying security roles and responsibilities;

(b) establish a procedure requiring the intervention of an authorised employee to enable/disable a remote access session; and

(c) review activity logs of each remote access session.

4.4.4.3 Dial-up Access

Systems accessible from dial-up terminals are particularly vulnerable to unauthorised access since the call can be initiated from virtually any telephone instrument. Official users of dial-up facilities must be distinguishable from public users if they are to be given access rights greater than those given to public users.

For services other than those authorised for the public, users of dial-up terminals shall be positively and uniquely identified and their identity authenticated (e.g., by password) to the systems being accessed.

For dial-up services other than those authorised for public use, the following should be considered:

(a) dial-up numbers should be unlisted and changed periodically;

(b) at a minimum, dial-up facilities should be provided with either:

   i. an automatic hang-up and call-back feature, with call-back to only pre-authorised numbers; or

   ii. authentication systems that employ smart card/token authentication.

(c) a port protection device (PPD) connected to communications ports of a host computer is typically capable of providing:

   i. authentication and access control decisions;

   ii. automatic hang-up and call-back to originator; and

   iii. attack signalling and event logging.

(d) security may be enhanced by instituting a two-person password procedure. One person's password gains access to the host and the other person's password gains access to the application. Under this procedure, neither acting alone can gain access to the application through dial-up; and

(e) a high level of dial-up security combines the call-back feature with either password authentication (an encryption key entered by the individual or smart card/token authentication) and terminal identification (an encryption key embedded in the hardware), with all data exchanged on-line being encrypted.

For dial-up facilities authorised for public use, take into consideration the following:

(a) systems which allow public access to the host computer require strengthened security at the operating system and applications level to reduce the likelihood of public intrusion into non-public applications. Such systems also should have the capability to monitor activity levels;

(b) ensure public usage does not unacceptably degrade system responsiveness for official functions; and

(c) systems which identify public users on the basis of communications port usage provide only minimal security since they are highly vulnerable to mistakes through erroneous hardware connections.

4.4.4.4 Virtual Private Networks

A virtual private network (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunnelling protocol and other security procedures. A VPN is similar to a system of owned or leased lines that can only be used by an organisation.

The idea of the VPN is motivated by the need for secure communication between computer networks in different locations with the same capabilities at much lower cost by using shared public infrastructure rather than a private one. This is especially important for government agencies that need connectivity between geographically distributed branch offices.

VPNs allow a trusted network to communicate with another trusted network over untrusted networks such as the Internet. Since some firewalls provide VPN capability, it is necessary to define the policy for establishing VPNs.

Any connection between firewalls over public networks shall use encrypted VPNs to ensure the privacy and integrity of the data passing over the public network. All VPN connections must be approved and managed by the System Administrator. Appropriate means for distributing and maintaining encryption keys must be established prior to operational use of VPNs.

Due to sharing of resources, a government agency that wishes to employ a VPN should have the following:

(a) a firewall located at a network gateway that protects the resources of a private network from users of other networks. Firewalls are implemented at the session layer of the network. This is to filter access and block unwanted users from the system. Therefore, government agencies should have defined policies, where change of policies are driven by the changing security requirements of those agencies;

(b) a firewall is installed in a specially designated computer separate from the rest of the network so that no incoming request can get directly at private network resources;

(c) allow to securely connect branch offices, telecommuters, mobile users, and selected parties to be securely connected to data resources by taking advantage of the cost effectiveness of the Internet; and

(d) remote users be given controlled access to selected servers (enforced path) and applications on the network or DMZ.

4.4.5 Connection with other Networks

With regard to other network connections some of the following should be undertaken to ensure ICT security is maintained:

(a) obtain specific authorisation from the ICTSO for connection to networks not under the organisation's control;

(b) establish written policies and procedures for connection to external networks; and

(c) impose on the security policy of the external provider requiring it to be verifiably as strong as the organisation's own network security policy.

Outside penetration or unauthorised access of the network can be prevented by:

(a) using fibre optics for internal cabling rather than the UTP cables because they are very difficult to interrupt or sniff (especially for very secure environment);

(b) minimising the installation of network protocols e.g. do not install NetBEUI on sub-netted networks, use TCP/IP & WINS servers instead;

(c) avoiding the use of Workgroups (i.e. disable workgroups). This is because workgroups support share-level security, but not user-level security. Organisations are advised to use Domains (LAN-Manager, NT) or NFS instead; and

(d) disabling floppy boot in PC client's BIOS set-up. Furthermore, PC clients should not be used as ftp or http servers.

4.4.5.1 Integrity of Connections

The capture of a session during accidental or intentional communication line drops can be prevented by:

(a) providing network controls for the detection and reporting of dropped communications lines and timely termination of all associated computer sessions; and

(b) adding a procedure that requires re-authentication when line drops occur.

4.4.5.2 Firewalls

The increased use of the Internet has made computer technology more useful but on the other hand, has resulted in the networking environment becoming more dangerous. This is because the Internet now also presents unprecedented opportunity for attack. Any computer user can subscribe to an Internet Service Provider (ISP) and become a true network 'node'. As a result there is no control over who can be on the Internet or what they use it for.

There is a dire need to protect systems on the Internet from both known and unknown assaults from a vast pool of attackers. What can generally be used to protect users from outside attacks can take the form of a firewall.

A firewall can be defined as a collection of components deployed between two networks that collectively have the following properties:

(a) all traffic from inside to outside, and vice-versa, must pass through the firewall; and

(b) only authorised traffic will be allowed to pass, as defined by the local ICT security policy.

A well-designed firewall is able to protect an organisation's network and ICT resources as well as those communicating partners' networks interconnected through the same firewall. Attacks from within the institution's network, or that of its communicating partner, must be addressed by using other security facilities.

Firewalls specified for use in a secure governmental institution should be designed for the following considerations:

(a) strong authentication and identification;

(b) a high degree of confidence of knowing who an institution is dealing with. A secure identification of the communication partner must precede any authorisation to conduct business. The ability of identifying who is using a system is required to prevent unauthorised use and to aid investigation of attacks;

(c) audit and archive requirements;

(d) the activity through a firewall contains information, which must be archived for a certain time to provide evidence, if necessary. Auditable security-related events also must be properly captured;

(e) availability;

(f) only reliable services should be provided;

(g) confidentiality; and

(h) confidence that governmental information will remain mandatorily protected.

Suggestions for proper selection and implementation of firewall

Due to the fact that the Internet environment is constantly changing, it is difficult to specify exhaustively all the requirements for firewalls. However, the following suggestions, where applicable, should form the basis of proper firewall selection and implementation:

(a) Technical Design Axioms

i. All connections to the institution's networks must be properly controlled;

ii. No IP packets will be exchanged between networks and the Internet except through the connection established through the firewall; and

iii. Traffic is exchanged through the firewall at the application layer only. Institution's hosts,which support incoming service requests from the public through the Internet will sit outside the firewall.

(b) Firewall Attributes

i The firewall systems will be implemented to work within the constraints of internal network routing technical features;

ii. The firewall must enforce a protocol discontinuity at the transport layer;

iii. The firewall must not switch any IP packets between the protected and unprotected networks;

iv. The firewall must hide the structure of the protected network;

v. The firewall must provide an audit trail of all communications to or through the firewall system and will generate alarms when suspicious activity is detected;

vi. The firewall system must use a ‘proxy server’ to provide application gateway function through the firewall;

vii. Routes through the firewall must be statically defined and the firewall configuration protected;

viii. The firewall must not accept session initiation from the public Internet;

ix. The firewall system must defend itself from direct attack;

x. The firewall must be structured so that there is no way to bypass any firewall component; and

xi. The firewall must include an application ‘launch server’ to support application connections from user systems to Internet services.

(c) Proxy Server Attributes

i. The proxy server acts as an application gateway;

ii. The proxy server hides internal details of the protected network from the public Internet;

iii. The proxy server does not switch any network level packets;

iv. The proxy server logs all activity in which it is involved; and

v. There are no user accounts on the proxy server itself.

(d) Launch Server Attributes (Web Based Application Server)

i. The launch server houses only client applications;

ii. User logins on the launch server must be different from the user’s ‘home account’; and

iii. Where possible, the launch server should be based on a hardware and software platform different from the user's home systems.

4.4.5.3 Public Users

Where public users are authorised access to networks or host systems, these public users as a class must be clearly identifiable and restricted to only services approved for public functions. Employees who have not been assigned a user identification code and means of authenticating their identity to the system are not distinguishable from public users and should not be afforded broader access.

4.4.5.4 Distributed Network Access

Owners of distributed information resources served by distributed networks shall prescribe sufficient controls to ensure that access to those resources is restricted to authorised users and uses only. These controls shall selectively limit services based on:

(a) user identification and authentication (e.g., password, smart card/ token);

(b) designation of other users, including the public where authorised, as a class (e.g., public access through dial-up or public switched networks), for the duration of a session; or

(c) physical access controls.

In a distributed network access to distributed processing systems and LAN, the following are recommended:

(a) authorisation at network entry should be made on the basis of valid user identification code and authentication (e.g., password, smart card/token) and should be provided under the framework of network services and controlled by the network management programme;

(b) network access should be controlled as close to the physical point of network entry as possible;

(c) connections between users on a network should be authorised by the host or the network node security manager programme, as appropriate;

(d) the designated manager of an independent network host serves the dual role as owner of the network system and as custodian of data under another's ownership while the data is being transported by the network;

(e) the host security management programme should maintain current user application activity authorisations through which each request must pass before a connection is made or a session is initiated;

(f) all unauthorised attempts (successful or otherwise) to access or modify data through a communication network should be promptly investigated; and

(g) if unauthorised access or modification of data occurs, the agency should promptly review its existing security system, including its internal policies and procedures. Appropriate corrective actions should be planned for and established to minimise or eliminate the possibility of recurrence. Employees may also need to be reminded of existing or revised procedures.

Government departments provide services to the public. In many cases members of the public require access to public sector ICT systems. In order to protect against unauthorised access from external users, the public domain information should be held separate (if possible) from corporate information. All access from external users is required to be routed through the department's firewall.

4.4.6 Protection during Transmission

Classified information must be prevented from disclosure during transmission by:

(a) encrypting classified information during electronic transmission; and

(b) protecting passwords by encryption during transmission, where possible.

Classified information must be protected from being corrupted or modified during transmission by authenticating information through approved digital signature.

4.4.6.1 Uploading & Downloading within Intranet

Uploading and downloading allow users to receive and send electronic files in a point-to-point manner. This service is developed to ease exchanging of document between two parties via electronic file transfer. It can create, replace, delete or copy document from one another.

Controls that should be implemented to protect uploading and downloading are as follows:

(a) Authorised User

Only authorised users are to perform uploading or downloading and this can be assured by restricting access to this service capability by logical access control;

(b) Physical Protection

The following can prevent destruction of information and information processing capability through access of equipment providing uploading and downloading services:

i. restricting physical access to information processing resources supplying uploading and downloading services;

ii. uploading and downloading services should reside in their own host;

iii. the service offered for external use should not be hosted in the same server or co-located with services offered for internal use; and

iv. uploading and downloading services for external use with weak or no security features should be prohibited.

4.4.6.2 Uploading & Downloading to/from the Internet

Uploading and downloading to/from the Internet is aimed at providing the capability to search for information related to business needs. Individuals and groups with such functions will be provided with Internet access capabilities.

4.4.7 Network Monitoring

Preventing exploitation of network vulnerabilities

Network vulnerabilities are those that can be exploited, whenever a system has the capability to electronically send information to or receive information from another system.

These vulnerabilities exist primarily in two areas:

(a) interception of information during transmission; and

(b) non-detection of improper messages and message headers received by the system.

Whenever the system is used to electronically send information to or receive information from another computer system, there is a chance that the information will be intercepted while en route. Therefore, steps should be taken to ensure that no information is compromised during transmission.

4.4.7.1 Problems to be Monitored

ICT based systems face new challenges not found under paper-based environment. Information been digital in nature is susceptible to a series of vulnerabilities such as:

(a) Trojan Horse and covert channel

i. Vulnerabilities

- disgruntled valid users;
- computer equipment is located in open areas;
- client stations are not password protected at boot time;

  when users are away from their computers, they tend to leave them still logged in to the network; and
- highly vulnerable network.

ii. Safeguards

- minimum reliability checks done on all employees;
- auditing of access to data;
- access to user accounts limited by client stations address (Novell feature); and
- ACLs are set in such a way that all the executables stored on the network can only be executed, i.e. they cannot be copied, deleted or modified.

(b) Eavesdropping

i. Vulnerabilities

- connections made with unshielded twisted-pair cables;
- no tempest or low emanation equipment used;
- monitors located beside windows;
- printers located in open areas and close to windows; and
- Ethernet topologies are used (data is broadcasted on network segments); and

ii. Safeguards

- physical access control; and
- fibre optics used.

(c) Virus on the Network

i. Vulnerabilities

- no virus scan or virus detection tool implemented;
- numerous uncontrolled external network connections via client stations;
- network start-up files are stored on each client stations; and
- placement of monitors/printers.

ii. Safeguards

- installation of virus scanning tools;
- access control features, which provide protection against unauthorised access to the network;
- weekly back-ups;
- security procedures such as stating that floppy diskettes external to the network should not be used on client stations; and
- encryption

(d) Intruders

Insiders and hackers are the main components of the human threat factor. Insiders are legitimate users of a system. When they use their access rights to circumvent security, this is known as an insider attack. Hackers, the most widely known human threat, are people who enjoy the challenge of breaking into systems.

(e) Insider Attacks

The primary threat to computer systems has traditionally been the insider attack. Insiders are likely to have specific goals and objectives, and have legitimate access to the system. Insiders can plant Trojan Horses or browse through the file system. This type of attack can be extremely difficult to detect or protect against.

The insider attack can affect all components of computer security. Browsing attacks the confidentiality of information on the system. Insiders can affect availability by overloading the system's processing or storage capacity, or by causing the system to crash.

These attacks are possible for a variety of reasons. On many systems, the access control settings for security-relevant objects do not reflect the organisation's security policy. This allows the insider to browse through sensitive data or plant Trojan Horses. The insider exploits operating system by planting bugs to cause amongst others the system to crash.

The actions are undetected because audit trails are inadequate or ignored.

(f) Hackers

The definition of the term 'hacker' has changed over the years. A hacker was once thought of as any individual who enjoyed getting the most out of the system he was using. A hacker would use a system extensively and study the system until he became proficient in all its nuances. This individual was respected as a source of information for local computer users; someone referred to as a 'guru' or 'wizard'. Now, however, the term hacker is used to refer to people who either break into systems for which they have no authorisation or intentionally overstep their bounds on systems for which they do not have legitimate access.

Methods used by hackers to gain unauthorised access to systems include:

i. password cracking;

ii. exploiting known security weaknesses;

iii. network spoofing; and

iv. 'social engineering'.

The most common techniques used to gain unauthorised system access involve password cracking and the exploitation of known security weaknesses. Password cracking is a technique used to surreptitiously gain system access by using another user's account. Users often select weak passwords. The two major sources of weaknesses in passwords are easily guessed passwords based on knowledge of the user (e.g. wife's maiden name) and passwords that are susceptible to dictionary attacks (i.e. brute-force guessing of passwords using a dictionary as the source of guesses).

Another method used to gain unauthorised system access is the exploitation of known security weaknesses. Two types of security weaknesses exist: configuration errors, and security bugs. There continues to be an increasing concern over configuration errors. Configuration errors occur when a system is set up in such a way that unwanted exposure is allowed. Then, according to the configuration, the system is at risk from even legitimate actions. An example of this would be that if a system 'exports' a file system to the world (makes the contents of a file system available to all other systems on the network), then any other machine can have full access to that file system (one major vendor ships systems with this configuration).

Security bugs occur when unexpected actions are allowed on the system due to a loophole in some application programme. An example would be sending a very long string of keystrokes to a screen-locking programme, thus causing the programme to crash and leaving the system inaccessible.

A third method of gaining unauthorised access is network spoofing. In network spoofing a system presents itself to the network as though it were a different system (system A impersonates system B by sending B's address instead of its own). The reason for doing this is that systems tend to operate within a group of other 'trusted' systems. Trust is imparted in a one-to-one fashion; system A trusts system B (this does not imply that system B trusts system A). Implied with this trust, is that the system administrator of the trusted system is performing his job properly and maintaining an appropriate level of security for his system. Network spoofing occurs in the following manner: if system A trusts system B and system C spoofs (impersonates) system B, then system C can gain otherwise denied access to system A.

‘Social engineering’ is the final method of gaining unauthorised system access. People have been known to call a system operator, pretending to be some authoritative figure and demanding that a password be changed to allow them access. One could also say that using personal data to guess a user’s password is social engineering.

4.4.7.2 How to Overcome Insider Attacks and Hackers

Today, desktop workstations are becoming the tool of more and more scientists and professionals. Without proper time and training to administer these systems, vulnerability to both internal and external attacks will increase. Workstations are usually administered by individuals whose primary job description is not the administration of the workstation. The workstation is merely a tool to assist in the performance of the actual job tasks. As a result, if the workstation is up and running, the individual is satisfied.

This neglectful and permissive attitude toward computer security can be very dangerous and has resulted in poor usage of controls and selection of easily guessed passwords. As these users become, in effect, workstation administrators, this problem will be compounded by configuration errors and a lax attitude towards security bugfixes. In order to correct this, systems should be designed so that security is the default and personnel should be equipped with adequate tools to verify that their systems are secure.

Of course, even with proper training and adequate tools threats will remain. New security bugs and attack mechanisms will be employed. Proper channels do not currently exist in most organisations for the dissemination of security related information. If organisations do not place a high enough priority on computer security, the average system will continue to be at risk from external threats.

System controls may not matched well to the average organisation’s security policy. As a direct result, the typical user is permitted to circumvent that policy on a frequent basis. The administrator is unable to enforce the policy because of the weak access controls, and cannot detect the violation of policy because of weak audit mechanisms. Even if the audit mechanisms are in place, the daunting volume of data produced makes it unlikely that the administrator will detect policy violations.

On-going research in integrity and intrusion detection promises to fill some of these gaps. Until these research projects become available as products, systems will remain vulnerable to internal threats.

Connectivity allows the hacker unlimited and virtually untraceable access to computer systems. Registering a network host is akin to listing the system’s modem phone numbers in the telephone directory. No one should do that without securing his or her modem lines (with dial-back modems or encryption units). Yet, most network hosts take no special security precautions for network access. They do not attempt to detect spoofing of systems; they do not limit the hosts that may access specific services.

A number of partial solutions to network security problems do exist. Examples include Kerberos, Secure NFS, RFC 931 authentication tools and ‘tcp wrapper’ programmes (access controls for network services with host granularity). However, these tools are not widely used because they are partial solutions or because they severely reduce functionality.

New solutions for organisations are becoming available, such as the Distributed Intrusion Detection System (DIDS) or filtering network gateways. DIDS monitors activities on a subnet. The filtering gateways are designed to enforce an organisation's network policy at the interface to the outside network. Such solutions may allow the organisation to enjoy most (if not all) of the benefits of network access and at the same time limit the hackers' access.

4.4.7.3 Monitoring Tools

Information disclosure, modification, or destruction by use of monitoring devices can be protected by:

(a) implementing use and storage controls over devices that monitor or record information being transmitted on a network (e.g., protocol analysers and Intrusion Detection System). The use of this equipment must have the consent of the ICTSO;

(b) ensuring that employees understand, as part of their condition of employment, that use of the organisation's information processing assets constitutes consent to monitoring; and

(c) continuing quality of controls must be ensured by maintaining an audit trail.

Many intrusion detection systems (IDS) base their operations on analysis of OS audit trails. This data forms a footprint of system usage over time. It is a convenient source of data and is readily available on most systems. From these observations, the IDS will compute metrics about the system's overall state, and decide whether an intrusion is currently occurring.

An IDS may also perform its own system monitoring. It may keep aggregate statistics, which give a system usage profile. These statistics can be derived from a variety of sources such as CPU usage, disk I/O, memory usage, activities by users, number of attempted logins, etc. These statistics must be continually updated to reflect the state of the current system state. They are correlated with an internal model which will allow the IDS to determine if a series of actions constitute a potential intrusion. This model may describe a set of intrusion scenarios or possibly encode the profile of a clean system.

An intrusion detection system should address the following issues, regardless of what mechanism it is based on:

(a) it must run continually without human supervision. The system must be reliable enough to allow it to run in the background of the system being observed. However, it should not be a 'black box'. That is, its internal workings should be examinable from outside;

(b) it must be fault tolerant in the sense that it must survive a system crash and not have its knowledge base rebuilt at restart;

(c) on a similar note to the above, it must resist subversion. The system can monitor itself to ensure that it has not been subverted;

(d) it must impose minimal overhead on the system. A system that slows a computer to a crawl will simply not be used;

(e) it must observe deviations from normal behaviour;

(f) it must be easily tailored to the system in question. Every system has a different usage pattern, and the defence mechanism should adapt easily to these patterns;

(g) it must cope with changing system behaviour over time as new applications are being added. The system profile will change over time, and the IDS must be able to adapt; and

(h) finally, it must be difficult to fool.

4.5 Security Posture Assessment of ICT

Security management is an on-going process

At anytime, the management of an organisation must be aware of the true level of its entire ICT security. This is because the security of a system is only as strong as its weakest point. No organisation should feel complacent about its state of security. There are continuously discovered vulnerabilities and bugs in operating system services, application software components, web browsers and e-mail systems.

What is a security posture assessment

The security state (posture) of an organisation must be assessed and a baseline established for continuous improvement. In the assessment process, existing policies (if any) and their implementation will be reviewed, installation validated and all points of entry into the network checked. Securing a system requires a proper set-up of all devices and services as well as the use of appropriate security tools. This is to minimise the risk of exposure to attacks through a non-technical approach such as social engineering that may defeat any technical means.

The security posture assessment (SPA) is performed to establish the current baseline security of the network and systems by discovering known vulnerabilities and weaknesses, with the intention of providing incremental improvements to tighten the security of the network and systems. The entire process can be divided into three (3) stages:

Stage 1: System/Network Architecture and Policy Review

Stage 2: System Testing and Network Penetration

Stage 3: Report/recommendation

Planning for a security posture assessment

Unless an organisation has the expertise and tools, an SPA exercise in the public sector could be outsourced to an independent 3rd party. The appointment of the consultant will conform to existing government procedures (*Pekeliling Perbendaharaan 3/95*). Care has to be taken since some information is highly sensitive and usually there are legal implications to be considered (for example the Official Secret Act 1972). An SPA starts with a rigorous and proper plan and this includes:

(a) obtaining the commitment of the management to allocate resources, e.g. documents about system architecture, network topology, application systems installed;

(b) requesting sufficient fund if the SPA is to be outsourced to an outside party;

(c) identifying contact persons in the organisation;

(d) establishing a communication plan during the SPA;

(e) establishing scope of the SPA (i.e. which computers, network devices and application systems will be included);

(f) scheduling the activity to minimise disruption of normal activity; and

(g) eventually detailing the day-to-day activities of the SPA exercise.

Finally, following submission of the SPA report, an organisation will seek to implement recommendations to improve its security level.

Note: The implementation stage is not part of the SPA exercise.

Chapter 5 LEGAL MATTERS

Despite its sophistication and complexities, ICT systems are vulnerable to abuse and threats. This may result in damage such as loss of confidentiality, information integrity, authenticity, availability, etc. Examples of threats to ICT environments are as listed in Appendix B.

Importance of cyber laws.

Cyber laws form an important component of the legal framework needed to facilitate the development of ICT systems by countering the threats and abuses related to such systems.

Cyber laws in response to ICT security requirements.

In relation to ICT security, cyber laws were enacted to:

(a) regulate and protect the ICT industry from misuse and illegal activities or activities that assist in the commissioning of illegal activities. Above all, cyber laws seek to promote the development of local ICT-based industries;

(b) describe in clear terms activities construed under the law as offences;

(c) describe in detail penalties for transgression; and

(d) provide soft infrastructure to lend support to the MSC initiative.

No.	***Act***	***Date of Royal Assent***	***Date of Publication in Gazette***	***Date of Enforcement***
1.	Digital Signature Act 1997	June 18, 1997	June 30, 1997	October 1, 1998
2.	Computer Crime Act 1997	June 18, 1997	June 30, 1997	June 1, 2000
3.	Telemedicine Act 1997	June 18, 1997	June 30, 1997	*
4.	Copyright (Amendment) Act 1997	June 18, 1997	June 30, 1997	April 1, 1999
5.	Communications & Multimedia Act 1998	September 23, 1998	October 15, 1998	April 1, 1999
6.	Malaysian Communications & Multimedia Commission Act 1998	September 23, 1998	October 15, 1998	April 1, 1999

* To be enforced

Table 5.1: Malaysian Cyber Laws

Other regulations related to computer crime.

In addition other existing regulations, which are related to computer crime include:

(a) Copyright Act 1987;

(b) Official Secrets Act 1972;

(c) Companies Act 1965 (Act 125);

(d) Trade Marks Act 1976;

(e) Patents Act 1983;

(f) Prison Act 1995; and

(g) Akta Arkib Negara 44/1996.

5.1 Cyber Laws and Legal Implications

5.1.1 Digital Signature Act 1997

Provision of the Digital Signature Act.

The Digital Signature Act was enacted to instill confidence and encourage the public to perform secured electronic transactions domestically as well as internationally. Under the Act, the digital signature provides a verification system to authenticate the identity of the author and verify the transmitted message.

Certificate must be obtained from Certification Authority.

For a digital signature to be recognised, it is necessary to obtain a certificate from a Certification Authority licensed by the Controller of Certification Authorities. On the salient elements of this law are that Certification Authorities authorised by a foreign government entity may be recognised and that the liability of a Certification Authority is limited. A document created in accordance with this Act or signed digitally is legally binding as a document.

Among the provisions of this Act are:

(a) the need for all Certification Authorities to be licensed;

(b) the appointment of a Controller of Certification Authorities;

(c) the main responsibility of a Controller of Certification Authorities is to license the Certification Authority;

(d) the main task of the Certification Authority is to verify the identity of subscribers;

(e) determination of the liability limits of the Certification Authorities and the legal effect of digital signatures; and

(f) delegation of authority to the Minister to appoint the Controller of Certification Authority.

5.1.2 Computer Crime Act 1997

Provision of Computer Crime Act.

The Computer Crime Act 1997 relates to offences due to the misuse of computers and complement existing criminal legislation. Under this law, unauthorised access/modification to any programme or data held in computer is an offence and will be penalised. This Act also has an effect outside Malaysia if the offences are committed by any person in any place outside Malaysia if the computer, programme or data is in Malaysia or capable of being connected to or used with a computer in Malaysia.

An abstract of the offences, punishment and enforcement under the Act are listed below:

List of Offences

Section	***Offences***
3	Unauthorised access to computer material
4	Unauthorised access with intent to commit or facilitate commission of further offence
5	Unauthorised modification of the contents of any computer
6	Wrongful communication
7	Abetments and attempts punishable as offences
8	Presumption
11	Obstruction of search

List of Punishment

Section	***Imprisonment***	***Fine***	***Or Both***
3	Not > 5 years	Not > RM 50,000.00	✓
4	Not > 10 years	Not > RM 150,000.00	✓
5	Not > 7 years; If cause injury, not > 10 years	Not > RM 100,000.00; If cause injury, Not > RM 150,000.00	✓
6	Not > 3 years	Not > RM 25,000.00	✓
7	Not > 1/2 of maximum term	Same amount as offences abetted	✓
11	Not > 3 years	Not > RM 25,000.00	✓

List of Enforcement

Section	***Offences***	***Search & Seizure***	***Arrest***
10	Powers of search, seizure & arrest	Person: not less than Inspector With or without warrant	Person: Any Police Officer. Without warrant (Seizable)

Table 5.2: List of Offences, Punishment and Enforcement

5.1.3 Telemedicine Act 1997

Provision of the Telemedicine Act.

The Telemedicine Act was enacted to provide the regulatory framework for the practice of Telemedicine and to recognise the use of multimedia in the practice of medicine.

Telemedicine can be practiced by a licensed personnel.

Telemedicine can be practiced by a local doctor who has a valid practicing certificate, a foreign licensed/registered doctor who has been certified by the Malaysian Medical Council through a local doctor or provisionally registered medical practitioner, medical assistant, nurse and midwife approved by the Director-General of Health. No other person can practice Telemedicine and offenders will be fined accordingly. The important condition in telemedicine is that the doctor must obtain written consent from the patient for such treatments. However, there is no provision in the Telemedicine Act on the liability of telemedicine practitioners. Liability is to be determined by tortuous or contractual principles.

Provision of Copyright (Amendment) Act.

5.1.4 Copyright (Amendment) Act 1997

This Act is to enhance copyright protection by taking into account development in information technology and the latest developments related to copyright under the World Intellectual Property Ownership (WIPO) Copyright Treaty 1996. The scope of copyright protection has been widened where an author is also given exclusive right of control. New copyright infringements and offences have been further identified and regulated under this Act.

An abstract of the offences, punishment and enforcement under the Act are listed below:

List of Offences

Section	***Offences***
41(1)(h)	Circumvents or causes the circumvention of any effective technological measures referred to in S.36 (3)
41(1)(i)	Removes or alters any electronic rights management information without authority
41(1)(j)	Distributes, imports for distribution or communicates to the public, without authority, works or copies of works in respect of which electronic rights management information has been removed or altered without authority

List of Punishment

Section	***Imprisonment***	***Fine (RM)***	***Or Both***
41(1)(h)	Not > 3 years Subsequent offence not > 5 years	Not > RM 250,000.00, Subsequent offence not > RM 500,000.00	✔
41(1)(i)	Not > 3 years Subsequent offence not > 5 years	Not > RM 250,000.00 Subsequent offence not > 500,000.00	✔
41(1)(j)	Not > 3 years; Subsequent Offence not > 5 years	Not > RM 250,000.00; Subsequent offence not RM 500,000.00	✔

List of Enforcement

Section	***Offences***	***Investigation***	***Search & Seizure***	***Arrest***
44	Entry by warrant or otherwise	-	Police not less than Inspector or Assistant Controller	-
50	Power of investigation	Police not less than Inspector or Assistant Controller	-	(Special power investigation) Police -without warrant Assistant Controller - with warrant

Table 5.3: List of Offences, Punishment and Enforcement

5.1.5 Communications and Multimedia Act 1998

Provision of the Communication and Multimedia Act.

This Act covers communications over the electronic media (exclusion of print media) and does not affect the application of existing laws on national security, illegal content, defamation and copyright. This Act, regulates various activities such as network facilities providers, network service providers, application service providers and content application services providers. Under this Act, the Minister is given the flexibility to grant licences for particular types of activity as he deems fit. This flexibility is to address of the changing requirements as the industry evolves.

5.1.6 Malaysian Communications & Multimedia Commission Act 1998

Provision of the Malaysian Communications and Multimedia Commission Act.

This Act provides the establishment of the Malaysian Communications and Multimedia Commission with powers to supervise and regulate the communications and multimedia activities in Malaysia, to enforce the communications and multimedia laws of Malaysia, and for related matters.

5.2 Crime Investigation

Increasing ICT security incidents.

Global trends indicate that ICT security incidents (fraud, theft, impersonation, loss of business opportunity, etc.) are increasing.

This is primarily due to:

(a) readily available facilities and tools plus the lack of control in their use;

(b) relatively easy in mounting attacks from a distance; and

(c) availability of valuable information on networks that could be exploited.

It is imperative that public sector officers involved in ICT security are aware of such incidents so as to enable them to mitigate risk and exposure of their respective ICT installations, including issues dealing with investigations and enforcement.

Few convictions due to grey areas.

Telecommunications fraud, computer-related crime incidents, investigations and computer forensics involve sciences affected by many external factors, such as continued advancements in technology, societal issues and legal issues. Most of the cases are esoteric in nature and there have been very few prosecutions and even fewer convictions being made. This is because of the many grey areas to be sorted out and tested through the courts. Until then, system attackers will have an advantage and computer abuse will continue to increase.

5.2.1 Definition of Computer Crime

Computer crime is a criminal act.

Computer crime is defined by the Royal Malaysian Police as:

(a) a criminal act in which a computer is **essential** to the perpetration of the crime; or

(b) a criminal act where a computer, **non-essential** to the perpetration of the crime, acts as a store of information concerning the crime.

5.2.1.1 Examples of Computer Essentials

Examples of computer essentials.

Some examples of computer essentials are:

(a) information theft via hacking;

(b) electronic funds transfer fraud;

(c) distribution of pornography via Internet;

(d) internet cash fraud; and

(e) credit card fraud.

Copyright MAMPU

5.2.1.2 Examples of Computer Non-Essentials

Examples of computer non-essential.

Some examples of computer non-essentials are:

- *(a)* all types of fraud;
- *(b)* murder;
- *(c)* theft;
- *(d)* forgery; and
- *(e)* potentially any type of crime.

5.2.2 Evidence

Computer related crime evidence is intangible and may differ from traditional forms.

Evidence is defined as anything offered in court to prove the truth or falsity of a fact in issue. However, evidence presented in a computer-related crime case may differ from traditional forms of evidence because in most cases the computer-related crime evidence is intangible. As a consequence, the legal problems of computer-based evidence are intensified and complex.

5.2.2.1 Types of Evidence

Different type of computer related crime evidence.

The most common forms of evidence that can be offered in court to prove the truth or falsity of a given fact are:

- *(a)* direct evidence is oral testimony obtained from any of the witness's five senses and is in itself proof or disproof of a fact in issue (e.g., an eyewitness statement);
- *(b)* real evidence also known as associative or physical evidence. It is made up of any tangible objects that prove or disprove guilt;
- *(c)* documentary evidence is evidence presented in the form of e.g. business records, manuals, and printouts. Much of the evidence submitted in a computer crime case is documentary evidence;
- *(d)* demonstrative evidence is evidence in the form of a model, experiment, chart, or an illustration offered as proof;
- *(e)* physical evidence includes tools used in the crime, fruits of the crime, or perishable evidence capable of reproduction to link the suspect to the crime; and
- *(f)* computer generated evidence such as:
  - i. visual output on the monitor;
  - ii. printed evidence on a printer/plotter;
  - iii. film recorder (i.e., a magnetic representation on disk and optical representation on CD); and
  - iv. data and information stored electronically on storage devices (e.g. diskettes, CD's, tapes, cartridges etc.).

5.2.3 Conducting Computer Crime Investigation

Immediately start the investigation after the report is made.

The computer crime investigation should start immediately following the report of any alleged transgression or criminal activity. The incident response plan will help set the objective of the investigation and will identify each of the steps in the investigative process.

5.2.3.1 Detection and Containment

Steps to be followed before the investigation.

Before any investigation, the following steps should be taken:

(a) the system intrusion or abusive conduct must first be detected. Swift detection of the actual intrusion not only helps to minimise system damage, but also assists in the identification of potential suspects;

(b) proactive and automated detection techniques must be instituted to minimise the amount of system damage in the wake of an attack; and

(c) once an incident is detected, it is essential to minimise the risk of any further loss by shutting down the system and reloading clean copies of the operating system and application programmes. However, failure to contain a known situation (i.e. a system penetration) may result in increased liability for the victim's organisation.

5.2.3.2 Report to Management

ICT incidents should be reported to the management immediately

All incidents should be reported to management as soon as possible. Prompt internal reporting is imperative to collect and preserve potential evidence. It is important that information about the investigation be limited to as few people as possible. Information should be given on a need-to-know basis, which limits the possibility of the investigation being leaked. E-mail should not be used to discuss the investigation on a compromised system.

Also, ICT incidents should be reported to the relevant parties.

Based on the type of crime and type of organisation it may be necessary to notify:

(a) CIO;

(b) MAMPU;

(c) The Office of the Government Chief Security Officer, Prime Minister's Department;

(d) The Audit Department, Prime Minister's Department;

(e) The Legal Affairs Division, Prime Minister's Department; and

(f) The Attorney-General's Department, Prime Minister's Department.

5.2.3.3 The Preliminary Investigation

Preliminary investigation proses

The preliminary investigation usually involves the following:

(a) a review of the initial complaint, inspection of the alleged damage or abuse, witness interviews, and, finally, examination of the system logs;

(b) the investigator must address the basic elements of the crime to determine the chances of successfully prosecuting a suspect either via civil or criminal action;

(c) the investigator must identify the requirements of the investigation (i.e., the financial implication and resources); and

(d) the investigator should not confront or talk with the suspect. Doing so would only give the suspect the opportunity to hide or destroy evidence.

5.2.3.4 Determine if Disclosure is Required

Determine if disclosure is required

It is important to determine if a disclosure is required or warranted under specific laws or regulations. Even if disclosure is not required, it is sometimes better to disclose the attack to possibly deter future attacks.

5.2.3.5 Investigation Considerations

Factors to consider when deciding to further investigate

There are many factors to consider when deciding whether to further investigate an alleged computer crime.

The investigation considerations are:

(a) the cost associated with an investigation;

(b) the effect on operations or the effect on the organisation's reputation; and

(c) the victim organisation must answer these questions:

  i. will productivity be stifled by the inquiry process?;

  ii. will the compromised system have to be shut down to conduct an examination of the evidence or crime scene?;

  iii. will any of the system components be held as evidence?;

  iv. will proprietary data be subject to disclosure?;

  v. will there be any increased exposure for failing to meet a 'standard of due care?';

  vi. will there be any potential adverse publicity related to the loss?; and

  vii. will a disclosure invite other perpetrators to commit similar acts, or will an investigation and subsequent prosecution deter future attacks?.

5.2.3.6 Who Should Conduct the Investigation?

Based on the type of investigation (i.e., civil, criminal, or insurance) and extent of the abuse, the victim must decide who is to conduct the investigation.

Victim is able to decide on the conducting party

The victim must choose from these options:

(a) conduct an internal investigation;

(b) bring in MAMPU to assess the damage, preserve evidence and provide recommendation for further action (refer to Appendix H: *Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)*); and

(c) bring in law enforcement officials.

Issue affecting are information dissemination, investigation control, cost and legality

The major issues affecting the decision as to which parties to bring (in order of priority) are information dissemination, investigative control, cost, and the associated legal issues. Once an incident is reported to law enforcement, information dissemination becomes uncontrolled. Law enforcement controls the entire investigation, from beginning to end. This does not always have a negative effect, but the victim organisation may have a different set of priorities.

Cost is of concern to conduct the investigation.

Cost is always a concern, and the investigation costs only add to the loss initially sustained by the attack or abuse. Even law enforcement agencies, which are normally considered “free”, add to the costs because of the technical assistance that they require during the investigation.

There are advantages and disadvantages for each of these groups previously identified. Internal investigators know the victim’s systems best, but may lack some of the legal and forensic training. Private investigators who specialise in high-technology crime also have a number of advantages, but usually involve higher costs. Private security practitioners and private investigators are also private businesses and may be more sensitive to business resumption than law enforcement.

Police involvement.

If the victim organisation decides to report to the police, care must be taken not to alert the perpetrator. When a police report is made the incident will become part of a public record. Now, there will no longer be on avenue for discretionary dissemination of information or a covert investigation. Therefore it is suggested that the victim organisation should ask the police to meet with it in plainclothes. When they arrive at the workplace, they should be announced as consultants. Be aware that the local law enforcement agency may not be well equipped to handle high-tech crime. Usually local law enforcement has limited budgets and place emphasis on problems related to violent crime and drugs. Moreover, with technology changing so rapidly, most local law enforcement officers lack the technical training to adequately investigate an alleged intrusion.

The same problems hold true for the prosecution and the judiciary. In order to prosecute a case successfully, both the prosecutor and the judge must have a reasonable understanding of high-technology laws and the crime in question, which is not always the case. Moreover, many of the current laws are woefully inadequate. Even though an action may be morally and ethically wrong, it is still possible that no law is violated (e.g., the LaMacchia case). Even when a law that has been violated, many of these laws remain untested and lack precedence. Because of this, many prosecutors are reluctant to prosecute high-technology crime cases.

Some of the defences have been used and accepted.

Some of the lines of defences that have been used, and accepted by the judiciary, are:

(a) if an organisation has no system security or lax system security, that organisation is implying that no organisation concern exists. Thus, there should be no court concern;

(b) if a person is not informed that access is unauthorised, it can be used as a defence; and

(c) if employees are not briefed and do not acknowledge understanding of policy, standards and procedures, they can use it as a defence.

Appendix A

KERAJAAN MALAYSIA

PEKELILING AM BIL. 3 TAHUN 2000

RANGKA DASAR KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI KERAJAAN

JABATAN PERDANA MENTERI
MALAYSIA

Dikelilingkan kepada:

Semua Ketua Setiausaha Kementerian
Semua Ketua Jabatan Persekutuan
Semua Ketua Pengurusan Badan Berkanun Persekutuan
Semua Y.B. Setiausaha Kerajaan Negeri
Semua Ketua Pengurusan Pihak Berkuasa Tempatan

JABATAN PERDANA MENTERI MALAYSIA
KOMPLEKS JABATAN PERDANA MENTERI
PUSAT PENTADBIRAN KERAJAAN
PERSEKUTUAN
62502 PUTRAJAYA

Telefon : 603-88881957
Faks : 603-88883721

Rujukan Kami : UPTM (S) 159/526/1(2)
Tarikh : 1 Oktober 2000

Semua Ketua Setiausaha Kementerian
Semua Ketua Jabatan Persekutuan
Semua Ketua Pengurusan Badan Berkanun
Semua Y.B. Setiausaha Kerajaan Negeri
Semua Ketua Pengurusan Pihak Berkuasa Tempatan

PEKELILING AM BIL. 3 TAHUN 2000

RANGKA DASAR KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI KERAJAAN

TUJUAN

Pekeliling ini bertujuan untuk menjelaskan Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan serta perkara-perkara berkaitan yang perlu diberi pertimbangan dan diambil tindakan oleh agensi-agensi Kerajaan.

LATAR BELAKANG

2. Kerajaan sentiasa memberi perhatian terhadap keselamatan teknologi maklumat dan komunikasi *(information and communications technology)* atau ICT terutamanya dalam usaha menjayakan pembangunan dan pelaksanaan Aplikasi Perdana Koridor Raya Multimedia. Kerajaan juga sedar akan repositori maklumat semasa yang sangat besar dalam simpanannya, dan dijangka akan bertambah besar dengan terlaksananya projek Aplikasi Perdana yang diterajui Perkhidmatan Awam. Nilai serta kegunaan repositori maklumat juga dijangka akan terus meningkat hasil dari peningkatan pengguna yang bergantung kepada sistem ICT. Ini merupakan sebahagian daripada kesan ledakan pembangunan ICT yang telah mencorak budaya kerja serta cara penyampaian perkhidmatan Kerajaan kepada rakyat. Trend menunjukkan semakin banyak agensi Kerajaan mengubah hala kepada penggunaan ICT yang lebih meluas untuk mengurangkan kos operasi dan meningkatkan produktiviti dan kualiti perkhidmatan kepada pelanggan.

3. Pertumbuhan pesat penggunaan ICT di kalangan ini, terutama melalui kemudahan Internet, mendedahkan maklumat secara lebih luas dan ini memungkinkan berlakunya pencerobohan yang boleh mengakibatkan kebocoran maklumat rahsia rasmi dan maklumat rasmi Kerajaan. Keadaan ini jika tidak diberi perhatian rapi boleh menimbulkan masalah yang lebih besar di masa hadapan. Di samping itu perlu ada keseimbangan antara kawalan keselamatan yang terlalu ketat sehingga membatasi penyebaran maklumat penyampaian perkhidmatan, dengan kawalan yang terlalu longgar yang boleh memudaratkan keselamatan atau kepentingan Perkhidmatan Awam dan Negara.

4. Menyedari pentingnya usaha-usaha menjamin keselamatan ICT, satu rangka Dasar Keselamatan ICT Kerajaan telah digubal berpandukan kepada prinsip-prinsip keselamatan ICT yang kukuh, tanggungjawab terhadap keselamatan maklumat, kesedaran terhadap ancaman dan langkah-langkah peningkatan tahap keselamatan maklumat.

RANGKA DASAR KESELAMATAN ICT KERAJAAN

5. Rangka Dasar Keselamatan ICT ini dirumus bagi memenuhi keperluan penguatkuasaan, kawalan dan langkah-langkah yang menyeluruh untuk melindungi aset ICT Kerajaan. Perlindungan keselamatan ini perlu bersesuaian dengan nilai atau sensitiviti aset yang dimaksudkan. Ia juga perlu seimbang dengan kesan yang mungkin timbul akibat kegagalan perlindungan yang sesuai. Pernyataan dasar, prinsip, objektif dan skop dasar ini dijelaskan dalam lampiran kepada Pekeliling ini.

TANGGUNGJAWAB AGENSI

6. Semua agensi Kerajaan adalah dikehendaki mematuhi Rangka Dasar Keselamatan ICT Kerajaan dan melaksanakan tanggungjawab yang ditetapkan. Untuk maksud ini, semua Ketua Jabatan adalah diminta mengambil tindakan-tindakan berikut:

(a) Melantik seorang Pegawai Keselamatan ICT di kalangan pegawai kanan yang bertanggungjawab dalam melaksanakan tindakan-tindakan yang ditetapkan dalam Rangka Dasar Keselamatan ICT. Perlantikan pegawai ini dan sebarang pertukaran perlu dimaklumkan kepada MAMPU.

(*b)* Menyediakan semua infrastruktur keselamatan ICT menepati prinsip-prinsip keselamatan berpandukan Rangka Dasar Keselamatan ICT dan Arahan Keselamatan yang disediakan oleh Ketua Pegawai Keselamatan Kerajaan.

(c) Menyedia dan mengkaji semula dokumen infrastruktur keselamatan ICT bagi tujuan audit keselamatan ICT.

(*d)* Mengenal pasti bidang-bidang keselamatan ICT yang perlu diberi perhatian rapi dan mengambil tindakan segera mengatasinya.

(e) Memastikan tahap keselamatan ICT adalah terjamin setiap masa.

KHIDMAT NASIHAT

7. Sebarang kemusykilan berkaitan dengan Surat Pekeliling ini dan Rangka Dasar Keselamatan ICT Kerajaan bolehlah dirujuk kepada MAMPU, manakala kemusykilan berkaitan dengan Arahan Keselamatan hendaklah dirujuk kepada Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia.

TARIKH KUATKUASA

Surat Pekeliling ini berkuatkuasa mulai tarikh ia dikeluarkan.

(TAN SRI ABDUL HALIM BIN ALI)
Ketua Setiausaha Negara

Copyright MAMPU

(Lampiran kepada
Surat Perkeliling Am
Bil. 3 Tahun 2000)

RANGKA DASAR KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI KERAJAAN

Unit Permodenan Tadbiran dan
Perancangan Pengurusan Malaysia
(MAMPU)
Jabatan Perdana Menteri

PENGENALAN

Kerajaan sedar akan tanggung jawab untuk memastikan keselamatan aset teknologi maklumat dan komunikasi *(information and communications technology)*, ringkasnya ICT, yang dimiliki atau di bawah jagaan dan kawalannya. Ini termasuk semua data, peralatan, rangkaian dan kemudahan ICT. Tanggung jawab ini juga harus dipikul oleh ahli pentadbiran Kerajaan, penjawat awam atau sesiapa sahaja yang mengakses dan yang menggunakan aset ICT Kerajaan.

RASIONAL

2. Tujuan utama keselamatan ICT adalah untuk menjamin kesinambungan urusan Kerajaan dengan meminimumkan kesan insiden keselamatan. Keselamatan ICT berkait rapat dengan pelindungan maklumat dan aset ICT. Ini kerana komponen peralatan dan perisian yang merupakan sebahagian daripada aset ICT Kerajaan adalah pelaburan besar dan perlu dilindungi. Begitu juga dengan maklumat yang tersimpan di dalam sistem ICT. Ia amat berharga kerana banyak sumber yang telah digunakan untuk menghasilkannya dan sukar untuk dijana semula dalam jangkamasa yang singkat. Tambahan pula terdapat maklumat yang diproses oleh sistem ICT adalah sensitif dan terperingkat. Pendedahan tanpa kebenaran atau pembocoran rahsia boleh memudaratkan kepentingan negara. Sebarang penggunaan aset ICT kerajaan selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber Kerajaan.

3. Memandangkan pentingnya aset ICT Kerajaan dilindungi, maka satu Dasar Keselamatan ICT Kerajaan adalah perlu diwujudkan.

PERNYATAAN DASAR KESELAMATAN ICT KERAJAAN

4. Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Keselamatan adalah suatu proses yang berterusan. Ia melibatkan aktiviti berkala yang mesti dilakukan dari semasa ke semasa untuk menjamin keselamatan kerana ancaman dan kelemahan sentiasa berubah.

5. Keselamatan ICT adalah bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan ICT berkait rapat dengan pelindungan aset ICT. Terdapat empat (4) komponen asas keselamatan ICT, iaitu:

(a) Melindungi maklumat rahsia rasmi dan maklumat rasmi kerajaan dari capaian tanpa kuasa yang sah;

(b) Menjamin setiap maklumat adalah tepat dan sempurna;

(c) Mempastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan

(d) Mempastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

6. Dasar Keselamatan ICT Kerajaan merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk menjamin keselamatan maklumat tersebut dan kebolehsediaan kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

(a) Kerahsiaan—Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran.

(b) Integriti—Data dan maklumat hendaklah tepat, lengkap dan kemaskini. Ia hanya boleh diubah dengan cara yang dibenarkan.

(c) Tidak Boleh Disangkal—Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal.

(d) Kesahihan—Data dan maklumat hendaklah dijamin kesahihannya.

(e) Kebolehsediaan—Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

7. Selain itu, langkah-langkah ke arah keselamatan ICT hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan semula jadi aset ICT; ancaman yang wujud akibat daripada kelemahan tersebut; risiko yang mungkin timbul; dan langkah-langkah pencegahan sesuai yang boleh diambil untuk menangani risiko berkenaan.

PRINSIP-PRINSIP DASAR KESELAMATAN ICT KERAJAAN

8. Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT Kerajaan adalah seperti berikut:

(a) Akses atas dasar “perlu mengetahui”

(b) Hak akses minimum

(c) Akauntabiliti

(d) Pengasingan

(e) Pengauditan

(f) Pematuhan

(g) Pemulihan

(h) Saling bergantung

(a) **Akses Atas Dasar Perlu Mengetahui**

9. Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar “perlu mengetahui” sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan akses di bawah prinsip ini adalah berasaskan kepada klasifikasi maklumat dan tapisan keselamatan pengguna seperti berikut:

(i) ***Klasifikasi Maklumat***

Keselamatan ICT Kerajaan hendaklah mematuhi “Arahan Keselamatan” perenggan 53, muka surat 15, di mana maklumat dikategorikan kepada Rahsia Besar, Rahsia, Sulit dan Terhad. Data, bahan atau maklumat rasmi yang sensitif atau bersifat terperingkat perlu dilindungi dari pendedahan, dimanipulasi atau diubah semasa dalam penghantaran. Penggunaan kod dan tandatangan digital mesti dipertimbangkan bagi melindungi data yang dikirim secara elektronik. Dasar kawalan akses ke atas aplikasi atau sistem juga hendaklah mengikut klasifikasi maklumat yang sama, iaitu sama ada rahsia besar, rahsia, sulit atau terhad.

(ii) ***Tapisan Keselamatan Pengguna***

Dasar Keselamatan ICT Kerajaan adalah mematuhi prinsip bahawa pengguna boleh diberi kebenaran mengakses kategori maklumat tertentu setelah siasatan latarbelakang menunjukkan tiada sebab atau faktor untuk menghalang pengguna daripada berbuat demikian.

(b) **Hak Akses Minimum**

10. Hak akses kepada pengguna hanya diberi pada tahap set yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan khas adalah diperlukan untuk membolehkan pengguna mewujud, menyimpan, mengemaskini, mengubah atau membatalkan sesuatu data atau maklumat.

(c) **Akauntabiliti**

11. Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT kerajaan. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber ICT. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mampu menyokong kemudahan mengesan atau mengesah bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka.

12. Akauntabiliti atau tanggungjawab pengguna termasuklah:

(i) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan.

(ii) Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa.

(iii) Menentukan maklumat sedia untuk digunakan.

(iv) Menjaga kerahsiaan kata laluan.

(v) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan.

(vi) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan.

(vii) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

(d) **Pengasingan**

13. Prinsip pengasingan bermaksud bahawa semua tugas-tugas mewujud, memadam, kemaskini, mengubah dan mengesahkan data diasingkan. Ia bertujuan untuk mengelak akses yang tidak dibenarkan dan melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat, dimanipulasi dan seterusnya, mengekalkan integriti dan kebolehsediaan.

14. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian. Ia bertujuan untuk mengasingkan akses kepada domain kedua-dua kumpulan tersebut seperti akses kepada fail data, fail program, kemudahan sistem dan komunikasi, manakala pemisahan antara domain pula adalah untuk mengawal dan mengurus perubahan pada konfigurasi dan keperluan sistem.

15. Pada tahap minimum, semua sistem ICT perlu mengekalkan persekitaran operasi yang berasingan seperti berikut:

(i) Persekitaran pembangunan di mana sesuatu aplikasi dalam proses pembangunan.

(ii) Persekitaran penerimaan iaitu peringkat di mana sesuatu aplikasi diuji.

(iii) Persekitaran sebenar di mana aplikasi sedia untuk dioperasikan.

(e) **Pengauditan**

16. Pengauditan adalah tindakan untuk mengenalpasti insiden berkaitan keselamatan atau mengenalpasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Dengan itu, aset ICT seperti komputer, pelayan, *router, firewall,* dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail.* Pentingnya *audit trail* ini menjadi semakin ketara apabila wujud keperluan untuk mengenalpasti punca masalah atau ancaman kepada keselamatan ICT. Oleh itu, rekod audit hendaklah dilindungi dan tersedia untuk penilaian atau tindakan serta merta.

17. Pengauditan juga perlu dibuat ke atas rekod-rekod manual seperti dokumen operasi, nota serah tugas, kelulusan keluar pejabat, memorandum, borang kebenaran, surat kuasa, senarai inventori dan kemudahan akses log. Ini adalah kerana dalam kes-kes tertentu, dokumen ini diperlukan untuk menyokong *audit trail* sistem komputer.

18. Keseluruhannya, sistem pengauditan ini adalah penting dalam menjamin akauntabiliti. Antara lain, sistem ini dapat dirujuk bagi menentukan perkara-perkara berikut:

(i) Mengesan pematuhan atau perlanggaran keselamatan.

(ii) Menyediakan catatan peristiwa mengikut urutan masa yang boleh digunakan untuk mengesan punca berlakunya perlanggaran keselamatan.

(iii) Menyediakan bahan bukti bagi menentukan sama ada berlakunya perlanggaran keselamatan.

(f) Pematuhan

19. Pematuhan adalah merupakan prinsip penting dalam menghindar dan mengesan sebarang perlanggaran Dasar. Pematuhan kepada Dasar Keselamatan ICT Kerajaan boleh dicapai melalui tindakan berikut:

(i) Mewujud proses yang sistematik khususnya dalam menjamin keselamatan ICT untuk memantau dan menilai tahap pematuhan langkah-langkah keselamatan yang telah dikuatkuasakan.

(ii) Merumus pelan pematuhan untuk menangani sebarang kelemahan atau kekurangan langkah-langkah keselamatan ICT yang dikenalpasti.

(iii) Melaksana program pemantauan keselamatan secara berterusan untuk memastikan standard, prosedur dan garis panduan keselamatan dipatuhi.

(iv) Menguatkuasa amalan melapur sebarang peristiwa yang mengancam keselamatan ICT dan seterusnya mengambil tindakan pembetulan.

(g) Pemulihan

20. Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Antara lain, pemulihan boleh dilakukan melalui tindakan-tindakan berikut:

(i) Merumus dan menguji Pelan Pemulihan Bencana—*(Disaster Recovery Plan).*

(ii) Mengamalkan langkah-langkah membuat salinan data dan lain-lain amalan baik dalam penggunaan ICT seperti menghapuskan virus, langkah-langkah pencegahan kebakaran dan amalan *“clean desk”*.

(h) Saling Bergantung

21. Langkah-langkah keselamatan ICT yang berkesan memerlukan pematuhan kepada semua prinsip-prinsip di atas. Setiap prinsip adalah saling lengkap-melengkapi antara satu dengan lain. Dengan itu, tindakan mempelbagaikan pendekatan dalam menyusun dan mencorak sebanyak mungkin mekanisma keselamatan, dapat menjamin keselamatan yang maksimum. Prinsip saling bergantung meliputi beberapa peringkat di mana di tahap minimum, mengandungi langkah-langkah berikut:

(i) Sambungan kepada Internet—Semua komunikasi antara sistem ICT dengan sistem luar hendaklah melalui mekanisma pusat untuk mengurus, menguatkuasa dan mengawas sebarang bahaya keselamatan. Melalui sistem ini, semua trafik dalaman hendaklah melalui *gateway firewall* yang diurus secara berpusat. Semua trafik dari luar ke dalam hendaklah juga melalui laluan ini atau melalui kumpulan modem yang dikawal secara berpusat. Dengan itu, penggunaan modem dalaman tidak dibenarkan.

(ii) *Backbone* Rangkaian—*Backbone* rangkaian akan hanya mengendalikan trafik yang telah dikod untuk meminimumkan intipan.

(iii) Rangkaian Jabatan—Semua rangkaian jabatan akan dihubungkan ke *backbone* melalui *firewall* yang mana akan pula mengkod semua trafik di antara rangkaian jabatan dengan rangkaian di peringkat yang seterusnya atau pusat data.

(iv) Pelayan Jabatan—Semua data dan maklumat yang kritikal atau sensitif akan hanya disimpan di pelayan jabatan atau di pelayan yang diurus secara pusat. Ini akan meminimumkan pendedahan, pengubahan atau kecurian. Semua data dan maklumat sensitif akan dikodkan.

OBJEKTIF DASAR KESELAMATAN ICT KERAJAAN

22. Objektif utama Dasar Keselamatan ICT Kerajaan ialah seperti berikut:

(i) Memastikan kelancaran operasi Kerajaan dan meminimumkan kerosakan atau kemusnahan;

(ii) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat daripada kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi; dan

(iii) Mencegah salahguna atau kecurian aset ICT kerajaan.

23. Dasar Keselamatan ICT Kerajaan ini juga bertujuan memudahkan perkongsian maklumat sesuai dengan keperluan operasi kerajaan. Ini hanya boleh dicapai dengan memastikan semua aset ICT dilindungi.

SKOP DASAR KESELAMATAN ICT KERAJAAN

24. Sistem ICT Kerajaan terdiri daripada manusia, peralatan, perisian, telekomunikasi, kemudahan ICT dan data. Sistem ini adalah aset yang amat berharga di mana masyarakat, swasta dan juga Kerajaan bergantung untuk menjalankan urusan rasmi Kerajaan dengan lancar. Dengan itu, Dasar Keselamatan ICT Kerajaan menetapkan keperluan-keperluan asas berikut:

(i) Data dan maklumat hendaklah boleh diakses secara berterusan dengan cepat, tepat, mudah dan dengan cara yang boleh dipercayai. Ini adalah amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti.

(ii) Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta untuk melindungi kepentingan kerajaan, bisnes dan masyarakat.

25. Memandangkan sistem ICT sangat kompleks dan terdedah kepada kelemahan, ancaman dan risiko, adalah tidak mudah untuk memenuhi keperluan ini. Sistem ICT dan komponennya yang saling berhubungan dan bergantungan antara satu dengan lain kerapkali mewujudkan pelbagai kelemahan. Sesetengah risiko hanya menjadi kenyataan setelah masa berlalu manakala sesetengahnya timbul apabila berlaku perubahan. Walau bagaimanapun risiko seperti ini hendaklah dikenalpasti dan ditangani sewajarnya.

26. Bagi menangani risiko ini dari semasa ke semasa, Dasar Keselamatan ICT Kerajaan akan diperjelaskan lagi melalui pengeluaran Standard Keselamatan ICT yang mengandungi garis panduan serta langkah-langkah keselamatan ICT. Kegunaan kesemua dokumen ini secara bersepadu adalah disarankan. Ini adalah kerana pembentukan dasar, standard, garis panduan dan langkah-langkah keselamatan ini diorientasikan untuk melindungi kerahsiaan data, maklumat dan sebarang kesimpulan yang boleh dibuat daripadanya.

27. Bagi menentukan Sistem ICT ini terjamin keselamatannya sepanjang masa, Dasar Keselamatan ICT Kerajaan ini merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasuk, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran, dan yang dibuat salinan keselamatan ke dalam semua aset ICT. Ini akan dilakukan melalui penubuhan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut:

(i) Data dan Maklumat—Semua data dan maklumat yang disimpan atau digunakan dipelbagai media atau peralatan ICT.

(ii) Peralatan ICT—Semua peralatan komputer dan periferal seperti komputer peribadi, stesen kerja, kerangka utama dan alat-alat prasarana seperti *Uninterrupted Power Supply* (UPS), punca kuasa dan pendingin hawa.

(iii) Media Storan—Semua media storan dan peralatan yang berkaitan seperti disket, kartrij, CD-ROM, pita, cakera, pemacu cakera dan pemacu pita.

(iv) Komunikasi dan Peralatan Rangkaian—Semua peralatan berkaitan komunikasi seperti pelayan rangkaian, *gateway, bridge, router* dan peralatan PABX.

(v) Perisian—Semua perisian yang digunakan untuk mengendali, memproses, menyimpan, menjana dan mengirim maklumat. Ini meliputi semua perisian sistem, perisian utiliti, perisian rangkaian, program aplikasi, pangkalan data, fail program dan fail data.

(vi) Dokumentasi—Semua dokumentasi yang mengandungi maklumat berkaitan dengan penggunaan dan pemasangan peralatan dan perisian. Ia juga meliputi data dalam semua bentuk media seperti salinan kekal, salinan elektronik, *transparencies*, risalah dan *slides*.

(vii) Manusia—Semua pengguna yang dibenarkan termasuk pentadbir dan pengurus serta mereka yang bertanggungjawab terhadap keselamatan ICT.

(viii) Premis Komputer dan Komunikasi—semua kemudahan serta premis yang diguna untuk menempatkan perkara (i)-(vii) di atas.

28. Setiap perkara di atas perlu diberi perlindungan rapi. Sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai perlanggaran langkah-langkah keselamatan.

29. Di samping itu, Dasar Keselamatan ICT Kerajaan ini juga adalah saling lengkap-melengkapi dan perlu dilaksanakan secara konsisten dengan undang-undang dan peraturan yang sedia ada.

TANGGUNGJAWAB KETUA-KETUA JABATAN

30. Semua Ketua-ketua Jabatan perlu mematuhi Dasar Keselamatan ICT Kerajaan. Tugas dan tanggungjawab Ketua-ketua Jabatan adalah seperti berikut:

(i) Menentukan semua pegawai dan staf jabatan memahami keperluan standard, garis panduan, prosedur dan langkah keselamatan di bawah Dasar Keselamatan ICT Kerajaan.

(ii) Menentukan semua pegawai dan staf jabatan mematuhi standard, garis panduan, prosedur dan langkah keselamatan di bawah Dasar Keselamatan ICT Kerajaan. Tindakan sewajarnya hendaklah diambil apabila berlaku sebarang perlanggaran keselamatan.

(iii) Menjalankan penilaian risiko dan program keselamatan berpandukan kepada standard, garis panduan, prosedur dan langkah keselamatan ICT.

(iv) Mengadakan Pelan Rancangan Pematuhan yang bertujuan untuk mengurus risiko yang timbul akibat daripada ketidakpatuhan kepada standard, garis panduan, prosedur dan langkah keselamatan ICT.

(v) Melaporkan kepada MAMPU, Jabatan Perdana Menteri sebarang insiden perlanggaran keselamatan seperti kejadian-kejadian berikut:

- Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa.

- Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian.

- Kata laluan atau mekanisma kawalan sistem akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan.

- Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerapkali gagal dan komunikasi tersalah hantar.

- Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak diingini.

31. Tugas-tugas di atas hendaklah dilaksanakan oleh Pegawai Keselamatan ICT Jabatan yang bertanggungjawab kepada Ketua Pegawai Maklumat (CIO) sepertimana yang dilantik di bawah Arahan KSN Rujukan PM(S) 18114 Jld 13 (74) bertarikh 22 Mac 2000.

TANGGUNGJAWAB AGENSI PUSAT

32. Agensi pusat yang bertanggungjawab ke atas keselamatan ICT kerajaan adalah Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU), Jabatan Perdana Menteri. Tanggungjawab MAMPU adalah seperti berikut:

(i) Memberi pendedahan dan penjelasan mengenai Dasar Keselamatan ICT Kerajaan.

(ii) Mengemaskini Dasar Keselamatan ICT Kerajaan termasuk menetapkan standard, garis panduan, prosedur dan langkah keselamatan dari semasa ke semasa.

(iii) Menyediakan perkhidmatan berpusat untuk menerima laporan insiden keselamatan ICT, penyebaran maklumat dan pelarasan tindakan pembetulan.

(iv) Memantau pelaksanaan dan menguatkuasa Dasar Keselamatan ICT Kerajaan.

PINDAAN DAN KEMASKINI

33. Dasar Keselamatan ICT Kerajaan adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Dasar ini hendaklah dibaca bersama dokumen-dokumen mengenai standard, garis panduan, prosedur dan langkah keselamatan ICT Kerajaan yang akan dikeluarkan dari semasa ke semasa.

MAKLUMAT LANJUT

Sebarang pertanyaan mengenai kandungan dokumen ini atau permohonan untuk keterangan lanjut, boleh ditujukan kepada:

Unit Pemodenan Tadbiran Dan Perancangan Pengurusan Malaysia
(MAMPU) Jabatan Perdana Menteri
(Bahagian Keselamatan ICT Kerajaan)
Aras 6 Blok B2 Parcel B
Kompleks Jabatan Perdana Menteri
Pusat Pentadbiran Kerajaan Persekutuan
62502 PUTRAJAYA
Telefon: 03-8888 2250
Faks: 03-8888 3286
E-Mel: ictsec@mampu.gov.my

Rangka Dasar Keselamatan ICT Kerajaan ini juga boleh diakses di laman web MAMPU JPM (http://www.mampu.gov.my)

Appendix B

EXAMPLES OF COMMON THREATS

a. Errors and Omissions

Mistakes that can occur in daily business operations during the processing of information or data by users. Such mistakes could be due to incorrect data entry or programming error and these can pose a threat to the integrity of the data and the whole system. Examples are false data entry, data leakage, etc.

b. Fraud, Theft and Impersonation

Information that is stolen or used for fraudulent purposes. This criminal act can be committed either by individuals or a group, insiders/outsiders or former employees who still have access to the computer system (not terminated promptly). Examples include act of masquerading, computer theft, scavenging, etc.

c. Employee Sabotage

Actions by employees to destroy existing systems in retaliation or as vandalism. Examples:

- destroying hardware or facilities to ensure the unavailability of the ICT system such as network failure, unavailability of hardware parts to operate, etc.;
- destroying programmes or data to discontinue the operations of the ICT system;
- entering data incorrectly to make the ICT system produce incorrect data output;
- deleting data to ensure the unavailability of the data to produce an output; and
- installing programme bugs such as viruses into the ICT system

These could also happen if the system accounts of former employees are not terminated immediately.

d. Loss of Physical and Infrastructure Support

Loss due to catastrophe such as power failure, data communication failure, water leakage, fire, flood, civil disturbance, bomb threat, riots or strikes that can interrupt business operations. This results in ICT system downtime and interrupted business transactions. Examples are software piracy, piggybacking and tailgating, asynchronous attack, etc.

e. Malicious Hackers

These are criminal hackers that could be insiders and/or outsiders who break into the ICT system without authorisation. Usually a hacker is able to break into the ICT system either through telecommunications network equipment (e.g. router, switches, hub) and/or communication lines. Hackers are receiving more attention since they are skilled users of the language code to break into the ICT systems. Examples are logic bombs, scavenging, etc.

f. Malicious Code

These codes refer to viruses, worms, Trojan Horses, logic bombs, and other ‘uninvited’ programmes. They are transmitted through media such as diskette, CD and/or networks such as the internet and intranet. Even though there are many solutions such as scanning are available to detect and destroy the code, some are not effective. This is due to the fact that the code is becoming increasingly more complex everyday. Each solution is suitable for a specific or certain code only. Examples are Trojan Horses, computer virus, salami, superzapping, etc.

g. Industrial Espionage

The act of gathering proprietary data from private companies or the government for the purpose of aiding another company or government. Industrial espionage can be perpetrated either by companies seeking to improve their competitive advantage or by governments seeking to aid their domestic industries.

Foreign industrial espionage carried out by a government is often referred to as economic espionage. Since information is processed and stored on ICT systems, ICT security can help protect against such threats; it can do little, however, to reduce the threat of authorised employees selling that information.

The three most damaging types of stolen information are pricing information, manufacturing process information, and product development and specification information. Other types of information stolen include customer lists, basic research, sales data, personnel data, compensation data, cost data, proposals and strategic plans.

h. Foreign Government Espionage

In some instances, threats posed by foreign government intelligence services may be present. In addition to possible economic espionage, foreign intelligence services may target unclassified ICT systems to further their intelligence missions. Sensitive information that may be of interest include travel plans of senior officials, civil defence and emergency preparedness, manufacturing technologies, satellite data, personnel and payroll data, law enforcement, investigative and security files.

Appendix C

EXAMPLES OF COMMON ABUSES, METHODS AND DETECTION

1 **Eavesdropping and Spying Eavesdropping**

For example wiretapping and monitoring of radio frequency emanations.

Voice wiretapping methods
Observation
Tracing sources of equipment used

Spying

Inclusive of criminal acquisition of information by covert observation.

2 **Scanning**

The process of presenting information sequentially to an automated system for the identification of those items that receive a positive response (e.g., until a password is identified)

Printouts from demonstration programmes may be used to incriminate a suspect.

3 **Masquerading**

The process of assuming (an intruder) the identity of an authorised user after acquiring the user's ID information

Audit log analysis
Password violations
Observation
Report by person impersonated

4 **Piggyback and Tailgating**

Physical piggybacking is a method of accessing to controlled access areas where control is accomplished by electronically or mechanically locked doors. Electronic piggybacking can occur where individuals use terminals in an online computer system and the system automatically verifies identification. Tailgating is the process of connecting a computer user to a computer in the same session as and under the same identifier as another computer user, whose session has been interrupted.

Access observations
Interviewed witnesses
Examination of journals and logs
Out-of-sequence messages
Specialized computer programs that analyse characteristics of on line computer user accesses.

5 **False Data Entry**

The process of changing data before or during its input to computers (e.g. forging, misrepresenting, or counterfeiting documents; exchanging computer tapes or disks; keyboard entry falsification; failure to enter data; and neutralizing or avoiding controls)

Data comparison
Document validation
Manual controls
Audit log analysis
Computer validation
Report analysis
Computer output comparison
Integrity tests (e.g. value limits, logic consistencies, hash totals, cross foot and column totals and forged entry)

6	**Superzapping** A utility program used as a systems tool to bypass all controls and able to modify or disclose any program or computer-based data. Many program similar to Superzap are available for microcomputers as well. Such powerful utility programs which are used by system programmers and computer operators can be dangerous if it falls into the wrong hands.	Comparison of files with historical copies Discrepancies in output reports, as noted by recipients Examination of computer usage logs
7	**Scavenging** It is a process to obtain or reuse information that may be left after processing or residual data left in a computer or computer tapes or disks after job execution.	Tracing of discovered proprietary information back to its source Testing of an operating system to reveal residual data after job execution
8	**Trojan Horses** It is the process of making alteration or covert placement of computer instructions or data in a program so that the computer will perform unauthorized functions. It is the primary method used to insert instructions for other acts of abuse (e.g. logic bombs, salami attacks, and viruses). This is the most commonly used method in computer program-based frauds and sabotage.	Program code comparison Testing of suspected programs Tracing of unexpected events or possible gain from the act to suspected programs and perpetrators Examination of computer audit logs for suspicious programs or pertinent entries
9	**Computer Viruses** It is a set of computer instructions that can propagate copies of versions of itself into computer programs or data when it is executed within unauthorised programs.	The file size may increase when a virus attaches itself to the program or data in the file. An unexpected change in the time of last update of a program or file may indicate a recent unauthorized modification. If several executable programs have the same date or time in the last update field, they have been updated together, possibly by a virus. A sudden unexpected decrease in free disk space may indicate sabotage by a virus attack. Unexpected disk accesses, especially in the execution of programs that do not use overlays or large data files, may indicate virus activity
10	**Salami Techniques** It is an automated form of abuse involving Trojan Horses or secret execution of an unauthorised program that causes unnoticed or immaterial debiting of small amounts of assets from a large number of sources or accounts.	Detailed data analysis using a binary search Program comparison Transaction audits Observation of financial activities

11	**Trapdoors** It is a facility created by programmers to insert code that allows them to compromise the requirements of preventing unintended access to the computer operating systems and unauthorised insertion of modified code, during the debugging phases of program development and later during system maintenance and improvement.	Exhaustive testing Comparison of specification to performance Specific testing based on evidence
12	**Logic Bombs** It involves a set of instructions in a computer program periodically executed in a computer operating system that determines conditions\ or state of the computer. Such instructions would facilitate the perpetration of an unauthorised or malicious act.	Program code comparisons Testing of suspected programs Tracing of possible gains from the act
13	**Asynchronous Attacks** These attacks normally force the operating system to perform requested jobs simultaneously, which eventually forces the operating system to use up all the resources available.	System testing of suspected attack methods Repeat execution of a job under normal and secured circumstances
14	**Data Leakage** This type of computer crime involves the unauthorised removal of data or copies of data from a computer system or computer facility.	Discovery of stolen information Tracing computer storage media back to the computer facility
15	**Software Piracy** Piracy is the copying and use of computer programs illegally in violation of existing laws. Commercially purchased computer programs are protected by copyright and their use is restricted.	Observation of computer users Search of computer users' facilities and computers Testimony of legitimate computer program purchasers Receivers of copied computer programs
16	**Computer Theft** Computer theft, burglary, and sale of stolen microcomputers and components are severe problems because the value of the contents of stolen computers often exceeds the value of the hardware taken.	Cross check with ICT asset inventory Identification of equipment Observation Report by owner Audit log
17	**Use of Computer for Criminal Perpetration** Use of a computer as a tool in a criminal activity such as planning, data communications, or control or even simulating an existing process or modelling a planned method for carrying out a crime, or monitoring a crime (i.e. by the abuser) to guarantee the success of a crime can be carried out easily.	Investigation of possible computer use by suspects Identification of equipment

Appendix D

EXAMPLE OF CONTENTS LIST FOR AN AGENCY/DEPARTMENT ICT SECURITY POLICY

1. Introduction
   - 1.1 Overview
   - 1.2 Scope and Purpose of the ICT Security Policy
2. Security Objectives and Principles
   - 2.1 Objectives
   - 2.2 Principles
3. Security Organization/Infrastructure
   - 3.1 Responsibilities
   - 3.2 Security Policies
   - 3.3 Security Incident Reporting
4. IT Security/Risk Analysis and Management Strategy
   - 4.1 Introduction
   - 4.2 Risk Analysis and Management
   - 4.3 Security Compliance Checking
5. Information Sensitivity and Risks
   - 5.1 Introduction
   - 5.2 Information Marking Scheme
   - 5.3 Organization Information Overview
   - 5.4 Organization Information Values/ Sensitivity Levels
   - 5.5 Threats/Vulnerabilities/Risks Overview
6. Hardware and Software Security
   - 6.1 Identification and Authentication
   - 6.2 Access Control
   - 6.3 Accounting and Audit Trail
   - 6.4 Full Deletion
   - 6.5 Malicious Software
   - 6.6 PC Security
   - 6.7 Laptop Security

7. Communications Security
    - 7.1 Introduction
    - 7.2 The Networking Infrastructure
    - 7.3 Internet
    - 7.4 Encryption/Message Authentication

8. Physical Security
    - 8.1 Introduction
    - 8.2 Location of Facilities
    - 8.3 Building Security and Protection
    - 8.4 Protection of Building Services
    - 8.5 Protection of Supporting Services
    - 8.6 Unauthorised Occupation
    - 8.7 PC/Workstation Accessibility
    - 8.8 Access to Magnetic Media
    - 8.9 Protection of Staff
    - 8.10 Protection against the Spread of Fire
    - 8.11 Water/Liquid Protection
    - 8.12 Hazard Detection and Reporting
    - 8.13 Lightning Protection
    - 8.14 Protection of Equipment against Theft
    - 8.15 Protection of the Environment
    - 8.16 Service and Maintenance Control

9. Personnel Security
    - 9.1 Introduction
    - 9.2 Terms of Employment
    - 9.3 Security Awareness and Training
    - 9.4 Employees
    - 9.5 Self-employed People under Contract
    - 9.6 Third parties

10. Document/Media Security
    - 10.1 Introduction
    - 10.2 Document Security
    - 10.3 Storage of Media
    - 10.4 Disposal of Media

11. Business Continuity, including Contingency Planning/Disaster Recovery, Strategy and Plan(s)
    - 11.1 Introduction
    - 11.2 Back-Up
    - 11.3 Business Continuity Strategy
    - 11.4 Business Continuity Plan(s)
12. Telecommuting
13. Outsourcing Policy
    - 13.1 Introduction
    - 13.2 Security Requirements
14. Change Control
    - 14.1 Feedback
    - 14.2 Changes to the Security Policy
    - 14.3 Status of the Document

Source: ISO/IEC 13335 Part 3

Appendix E

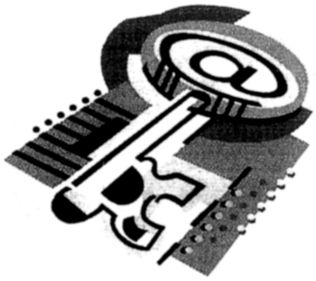
A SAMPLE ICT SECURITY RISK MANAGEMENT PROCESS

STEP 1
Set up a Risk Management Committee

STEP 2
Identify the security issues (threat or vulnerabilities) associated with the department ICT environment

STEP 3
Analyse the impact of those issues

STEP 4
Quantify the severity of the risks or identified their monetary impact



STEP 5
Identify the requirements or necessary safeguards and counter measures to reduce the impact of identified threats to an acceptable level

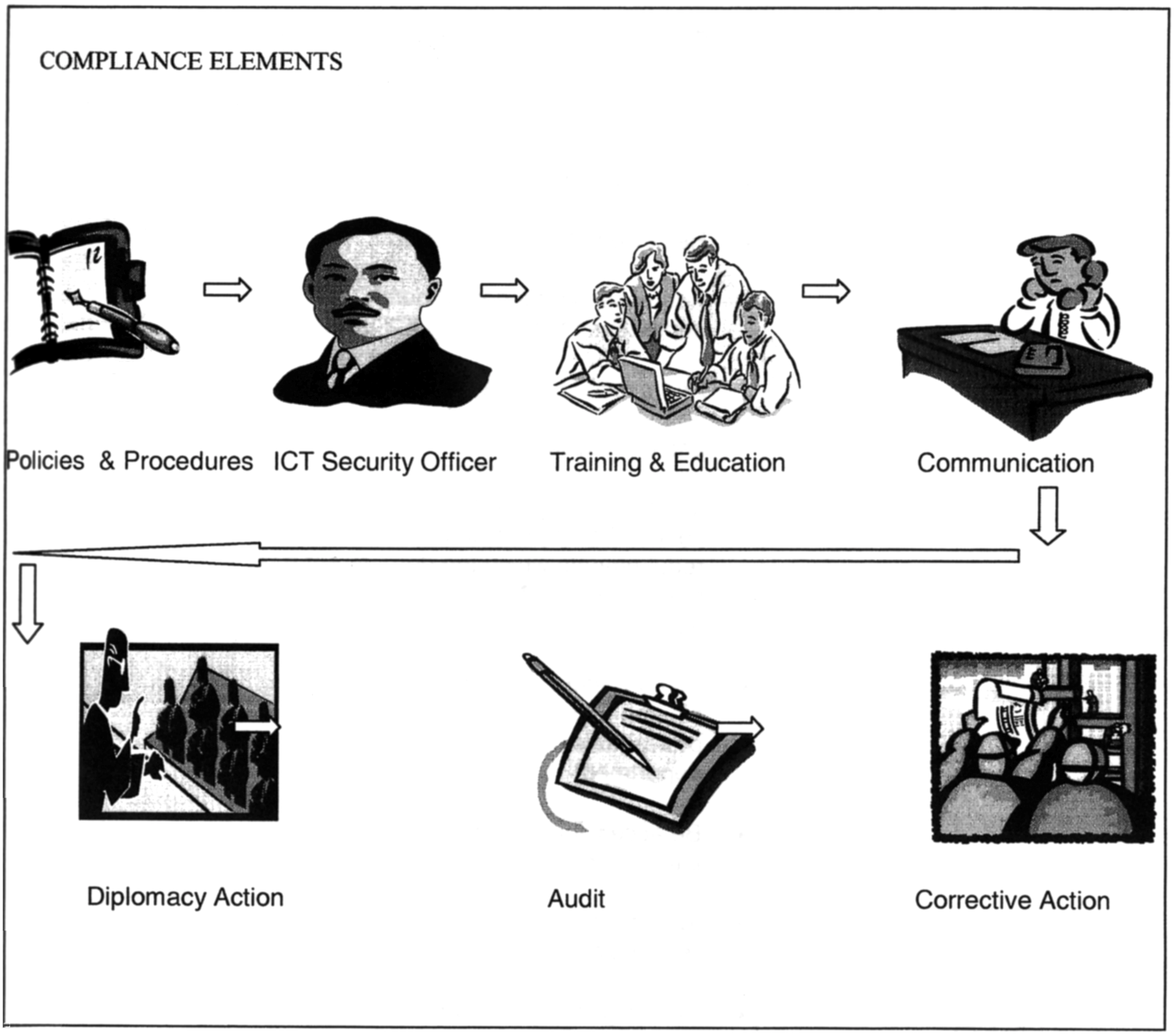
STEP 6
Implement safeguards and monitor effectiveness

STEP 7
Prepare risk management report and include residual risk and uncertainty analysis

Copyright MAMPU

Appendix F

A SAMPLE ICT SECURITY ADHERENCE COMPLIANCE PLAN



Compliance Checklist Plan

No.	Compliance Element	Compliance checklist	Yes	No
1.	**Policies and Procedures**	● Written and documented ● Adopted at the department level ● Approved by management ● Promulgated and communicated to all employees. ● State management commitment ● Reviewed at regular intervals ● Addressed in the department's approaches to managing ICT security ● Addressed in the department's operating procedures, business rules and employees' ethics. ● Identify any legislation, standards, codes of best practice or other external requirements which the department has to adhere to that affect its ICT applications ● Be consistent with ethical standards binding upon the occupations and professions of those employed by the department ● Be accessible and easily understood by intended readers ● Identify the ICTSO together with his/her responsibilities.		
2.	**ICTSO**	● Be assigned by management ● Be knowledgeable on ICT ● Have background, training or interest in compliance issues. ➢ Understand roles and responsibilities.		
3.	**Training and Education**	● Develop ➢ Training plan ➢ dentify audience ➢ Identify contents ➢ Implement and monitor the plan		

No.	Compliance Element	Compliance checklist	Yes	No
4.	**Communication**	● Establish Help Desk		
5.	**Disciplinary Action**	● Diplomacy actions taken		
6.	**Audit**	● Conduct internal audits at least once a year ● Identify non-compliance ● Report to CIO/ICTSO ● Use auditing tools		
7.	**Corrective Action**	● Reporting mechanisms ● Incident response handling ● Roles and responsibilities of various committees ● Recovery steps ● Business resumption plan		

Appendix G

A SAMPLE ICT STRATEGIC PLAN

THIS DOCUMENT

This document provides a template for the Agency ISP report. It provides further details on, and examples of, the documents that will make up the ISP report. Agencies are encouraged to adapt their existing tables and diagrams to present the requested information.

The table below provides a guide on the information being provided under each item.

▣	Information on the subject matter
⧈	Agency tasks. The information requested is the minimum expected and becomes less prescriptive in the later phases.
□	Agencies can provide further relevant information to support or clarify the subject matter
⬚	Examples
▭	Fixed Format Response

Acknowledgment: This template has been based upon the DMR Macroscope™.

GENERAL

Agency Name :

▭

Level ***(please tick relevant box):***

□	Federal Government
□	State Government
□	Statutory Body
□	Local Authority

Contact details for Person Responsible for ISP:

Name:	
Position:	
Address:	
Tel No :	Fax No:
Email id :	

PROJECT INITIATION

Project Plan

If there is an existing ISP and it has been updated or implemented within the last 12 months, then a copy of the ISP can be submitted to MAMPU to confirm sufficiency.

If the latest ISP is more than 12 months old, then there is a need to update it and provide the details as requested in the template.

Provide the schedule for the identified phases of the ISP.
Provide the Manpower plan to carry out the ISP.
The plan should be authorised by the Project Manager and have the approval of the Chairman of the IT Steering Committee.

Business Context Definition

Overview

This phase provides information on the current Agency and IT context that will provide the basis for the subsequent phases to build their observations and form their recommendations.

It is expected that each Agency has its own vision and mission statement that have been revised or updated within the last 12 months. Otherwise there is a need to confirm that these statements are still valid.

Mission Statement

Document the Agency’s existing Mission statement.
Describe any IT initiative or projects undertaken to support the Mission.

Vision statement

Document the Agency's existing Vision statement.

Describe any IT initiative or projects undertaken to support the Vision.

"Our vision is to be a world class performer and a Malaysian leader in providing <services in .....> and to be recognised as such by our customers and suppliers so we will satisfy our customer expectations for quality services at competitive prices."

VISION STATEMENT FOR THE MAINTENANCE FUNCTION

BUSINESS VISION	INFORMATION SYSTEM VISION
Autonomous work groups will be responsible for the maintenance of a group of assets	Systems will set the optimum maintenance date on the basis of the maintenance rules and the component's history
Maintenance personnel will be fewer in number but more highly trained and multi-skilled	The system will intelligently group the maintenance of related components
Periodic maintenance will be reduced in favour of on-condition maintenance	Set the actual maintenance date
Reliable and non-critical components will be subject to breakdown maintenance only	On-site maintenance will be assisted by local access to all relevant maintenance instructions and drawings in electronic form
	All data regarding the maintenance undertaken (labour, parts, modifications) will be captured on site

Identify the Strategic Drivers including the government and external environment

The Strategic Drivers are those things that must be done well if the mission and objectives of the Agency are to be achieved.

They represent critical points in the business where leverage may be available. IT may play a part in assisting some of these drivers. It is essential to know the role of IT in assisting these drivers.

Document the Agency's Strategic Drivers. These should cover business, the organisation and IT.

Describe any IT initiative or projects undertaken to support the Strategic Drivers.

The Agency Strategic Business Drivers were identified as:

- Implementation of customer driven business strategies and operations with emphasis on value adding customer service;
- Use of IT to optimise management of work and resources;
- Integration of strategic directions and initiatives with business operations, particularly in the co-ordination of change;
- Operating on a commercially competitive basis with commercial financial management practices;
- Alignment of Agency plans with the objectives and directions outlined within the Electronic Government Blueprint;
- Availability of a skilled and motivated work force with clear purpose, accountability and responsibility.

Business Environment—External

State the trends and issues in the Agency external environment (including the use of IT) for the identified areas :

Key products & services

Customers

Distribution or access channels e.g. information or products to be provided to clients or other agencies, or access channels to the Agencies services or products

Provide this information in a diagram, such as a context diagram. The diagram should show the Agency's supply chain (including other agencies), clients and other external organisations the Agency must deal with in order to deliver its mission.

State the key factors that need to be managed for the Agency to meet its business objectives.

Business Environment—Internal

It is expected that Agencies will have developed key measures that describe the size and extent of their operations, in addition to key performance indicators used to manage its operations.

Key performance indicators and trends

State the trends and targets for the Agency's main performance indicators. It should include financial targets (such as revenue, HR costs, IT expenses). Non-financial targets (such as client service level turnaround time) are also important.

SWOT analysis of support functions

A SWOT (strengths, weaknesses, opportunities and threats) analysis of the Agency's support functions covering areas such as organisations, human resources, technology and functional capabilities.

Findings from recent surveys and studies such as organisation reviews, etc.

> If there are any surveys or studies carried out in the last 2 years, provide a brief synopsis of the findings emphasising any implications of the strategy for IT.

Organisational Review

High-level business model

> This information can be illustrated by means of a context diagram showing the Agency's important functions and the information flows between them.

Functional roles & accountabilities

> Show the Agency organisation chart with a brief description of the accountabilities of each functional area. Include the reporting line for the IT organisation. List the key standing committees and their area of responsibility. Include the Chairman and the members.

Review of key management processes

> List the issues that each senior manager identifies that he/she would like to resolve to better achieve his/her business objectives.
>
> List the areas the senior managers identify could be more effective with IT support or improved IT service levels.
>
> Identify any external comparisons that provide 'best practice' measures on the Key Performance Indicators.

Capacity for Change

> This is to provide information on Agency readiness to implement change, which is required in order to transform the organisation. The readiness of the Agency will depend on the existing ability and experience of staff and management in relation to organisational change.
>
> Generally, if an organisation has been exposed to major change, then it will be better prepared to embark on the ISP migration plan and manage the risks involved.

> Identify any change programmes the Agency has carried out in the last 3 years including organisational restructuring, introduction of new processes and procedures and new IT projects.

IT Literacy

This is to provide an insight as to the IT knowledge of the Agency population, other than the IT department. Measures that describe IT literacy could include: the number of staff with a PC; number with access to PC; experience with managing a remote node of a network; non-IT staff involved with the integrity of the Agency data, the number of staff with MS Office skills, etc.

Provide measures that describe the IT literacy of the Agency staff and their key clients

BASELINE IT ASSESSMENT
Review of Current Information Technology Environment

Applications Portfolio

This is not restricted to classic MIS application systems, but includes all applications of IT to support business requirements (e.g. office technology, voice/image...). These applications might be applications developed by user departments other than IT

Identify existing application systems:

Big 10 : the 10 applications which make the most contribution to supporting the business, especially the strategic drivers

New 10: the 10 most recently developed applications, which make critical contributions to the business. These applications may or may not overlap with the Big 10,

Next 10: the projects currently underway which are intended to make critical contributions to the business.

For each application identified, provide :

- a short description of the application explaining its main functional areas and main group of users
- an assessment of its value to the Agency such as High, Medium or Low
- an assessment of the underlying IT Technology such as Leading Edge, Current or Out of date
- the number of master records for the application and the size of it’s database
- the number of transactions per day (Provide the volume for a relevant measurement period).

Technology penetration

Assess the level of IT investment and usage. Provide the following information :

- Amount of IT investment for Hardware & software for past 3 years
- Amount of IT expenses for Overhead (such as salary) for the past year
- No of employees in the whole organisation
- No of PCs not LAN connected
- No of LAN connected PCs
- Identify other terminal devices (e.g. VDUs, printers) and the number for each type
- No of Processors
- No of users with email access
- No of users with Internet access
- No of users with MS Office (Word, PowerPoint & Excel) skills.

IT organisation, resources and skills

Provide the existing IT organisation structure and headcount including the reporting channel to management and any outsourced services. Identify the number of permanent and contracting personnel in the organisation structure. Also include people outside the IT department but who do IT work or who have a working liaison with IT as part of their job.

Identify the existing experience and skills level.

Identify the typical IT projects carried out and whether they are implemented internally or with external assistance.

Provide an indication on the user satisfaction level to the IT range and quality of services.

IT management process

Listed are some examples of IT management processes.

Development and Maintenance e.g. applications planning, monitoring and control; data management, application/software development and upgrade, tuning and system balancing,

Management e.g. financial planning, monitoring and control,

Service Delivery e.g. service level management, security management

Resource Management e.g. capacity, skills

Resource Control e.g. change control

Service Control e.g. production and distribution scheduling,

Information Services e.g. production, distribution, network management

Identify the existing management processes being practised.

Indicate when the documented policy and procedures were last updated or reviewed.

Provide the Table of Contents for each of the documented internal management processes, which are being adhered to.

ISO 9000 accreditation

Identify the areas or processes, which the Agency have completed or are working towards ISO 9000 accreditation. For each of these areas, provide the following details:

- The current progress,
- The completed date or planned time frame in achieving the accreditation.
- IT Service Level Management
- Does service level agreement exist for:
- major applications,
- infrastructure (such as desktop and network),
- IT support.

If yes, summarise the key service levels for each of the above.

IT environment

It is expected that each Agency can provide high level, or Architecture diagrams that describe the IT environment. These would normally cover applications, data and IT infrastructure (Host, or network computers, networks, etc.)

Provide the Architecture Layer Diagrams for the Agency. At the very least, it should cover:
production environment,
development and testing environment.

Refer to Example 1 in Sample Diagrams.

Provide Network Diagrams for the Agency’s network which show:

- LAN,
- WAN,
- Connectivity to public networks,
- Connectivity to other external organisations and agencies
- Include information such as bandwidth, location topology and protocols.

Refer to Example 2 - 4 in Sample Diagrams.

Strategic Directions

Summary

Based on the analysis of the corporate strategies, business drivers and the current business and IT assessment, develop the agreed model of the transformed organisation. This may require the use of business process re-engineering (BPR) techniques.

The transformed organisation

Provide the model(s) which describe the transformed organisation.
Describe the changes in the Agency, its business practices, supply & delivery channels, etc. required to satisfy the strategic drivers.

Role of Information Technology in supporting the new organisation

Determine the business drivers for IT that will drive changes to the IT organisation, its business practices, its services and if necessary, its IT infrastructure.

Implications of IT for the new organisation

Determine the changes IT will need to undergo in order to support the transformed organisation

Opportunity Areas

Determine the immediate opportunity areas in which IT can provide leverage to the business

Copyright MAMPU

IT OPPORTUNITY Qualification

Summary

This phase builds on the work of the Strategic Directions and identifies all the IT opportunities to support the Agency to achieve its target. These opportunities should be assessed against the reality of IT services, facilities and staff capability, the business priority and the resulting benefits. This phase will produce the list of IT projects to be carried out through the ISP.

Summary of projects identified, concentrating on business case aspects

Provide a summary list of identified IT projects in a table with an assessment of:

- Strategic value to Agency
- Benefits to be delivered
- Costs
- Priority
- Risk
- Implementation impact
- IT impact
- EG alignment.

Summary of cost/benefit analyses

Provide a summary list of identified IT projects and their projected costs and benefits, both tangible and intangible.

Project Definition (to be treated for each recommended project)

For each recommended project provide :

- Project overview
- New environment scenario
- Project Objective
- Target user groups
- Resources required (people, costs, other,.....)
- Architectural implications
- Technical feasibility
- Key dependencies
- Overall schedule
- Expected benefits
- Cost estimates
- Risk assessment
- Impact assessment

Copyright MAMPU

Deferred Projects

Provide a list of the deferred projects with the following:

- Description of deferred project
- Reasons for deferment
- Plans for re-examination

TARGET IT INFRASTRUCTURE

Vision for Information Technology

The IT vision will be based upon the findings of the Baseline IT assessment and the business vision. It will describe the changes that IT management will need to implement to support the transformed organisation. This deliverable will provide the focus for IT projects during the ISP timeframe

Provide the Agency IT vision and mission statement to support the transformed organisation.

Provide a summary of the IT support required for the transformed organisation.

Describe the key IT policies and principles.

List the IT business drivers.

List the IT organisational changes required.

IT Group aim to be:

- A strategic asset that is flexible and enhances the Agency's opportunities for growth and business performance.
- A fundamental part of business re-engineering and total quality processes - a facilitator and catalyst of change - providing managed leverage and value add to the business.
- Demonstrate support for EG polices and directions through the submission of aligned projects for funding.
- Managed as a business issue not a technical one.
- Supplied by value adding service and product suppliers both internal and external to the Agency working in partnership with the business.
- Meeting the balanced and justified needs of both the Agency and its operating units.
- An area where the Agency excels and focuses on the application of Information Technology for business advantage.
- Clearly enjoying the benefits of consistency with IT standards and policies, which are manifested in enhanced flexibility, cost efficiency and effectiveness, managed risk and business advantage.

Information Technology Infrastructure

Applications Portfolio

Provide a list of the application systems according to the following grouping :

- Prime business applications—which support the Agency business objectives and EG's objectives
- Internal management applications—which support internal management such as HR, project management
- Support applications such as word processing, workflow, e-mail, document management.
- Provide high-level diagrams of applications for the target organisation showing the applications and their interfaces, including applications of external agencies and organisations, if appropriate.

Data model

Provide a high level Data Model at the "data subject" level to show the information base of the transformed organisation.

IT Delivery Model

Provide the following diagrams to show what and how IT will be delivered to the users :

- Architecture Layer Diagrams
- Network Diagrams
- Technology Zone Map

(Refer to the requirement for the current IT environment in Section 6).

IT Management
IT Organisation & Manpower

This phase defines the IT management structure, practices and skills, etc. to support the transformed organisation.

IT Steering Committee

If there is no existing IT Steering Committee, indicate whether there are any plans to establish such a Committee and when it will be set up.

IT Organisation Chart

Provide the target IT organisation structure to support the transformed organisation.

Indicate the user access channels to obtain support.

Provide the critical support departments that are required to work with IT or to support IT (e.g. Business Process Management, Systems & Methods).

Provide the strategies such as internally provided system integrators or outsourcing, etc for the Agency to provide the required support.

IT Skills Required

Identify the IT skills required to support the target IT organisation and how the agency plan to equip itself with the required skill set. Information needed include :

- Skills required,
- Is it available internally,
- How to obtain the skills required. (e.g. recruitment, internal development, use of consultants, outsourcing).

Headcounts

Indicate the number of personnel estimated to staff the target IT and any new support departments.

Service Level Management

Describe :

- IT services required,
- Service level targets.

IT Management Processes (defined for each key process with recommended changes)

Provide a description of the IT Management processes to be implemented. Include :

- Purpose of the process,
- Stakeholders,
- Proposed changes.

Migration Planning
Summary

The Migration Plan for the ISP period sets out the projects and time frame that will move the Agency from its current state to the transformed organisation.

Provide:

- A summary of the Migration Plan,
- Brief overview of objectives, key agency objectives and migration strategy.
- Brief description of key projects (objective/deliverable, delivery date, cost/benefit, significant risk issues).

Financial Summary

Provide a table of recommended projects with their cost benefit information.

Implementation Strategy

Provide the implementation strategy including :

- Summary of target environment (overall organisation and IT environment),
- Major migration objectives for next 3 to 5 years,
- Approach and phases to migrate to target environment,
- Change management issues and recommendations.

Projects Schedule (For next 3 to 5 years)

Provide a Gantt chart, which shows a schedule of all recommended projects. Include the IT management initiatives identified during the IT Management phase.

EXECUTIVE SUMMARY

Executive Summary

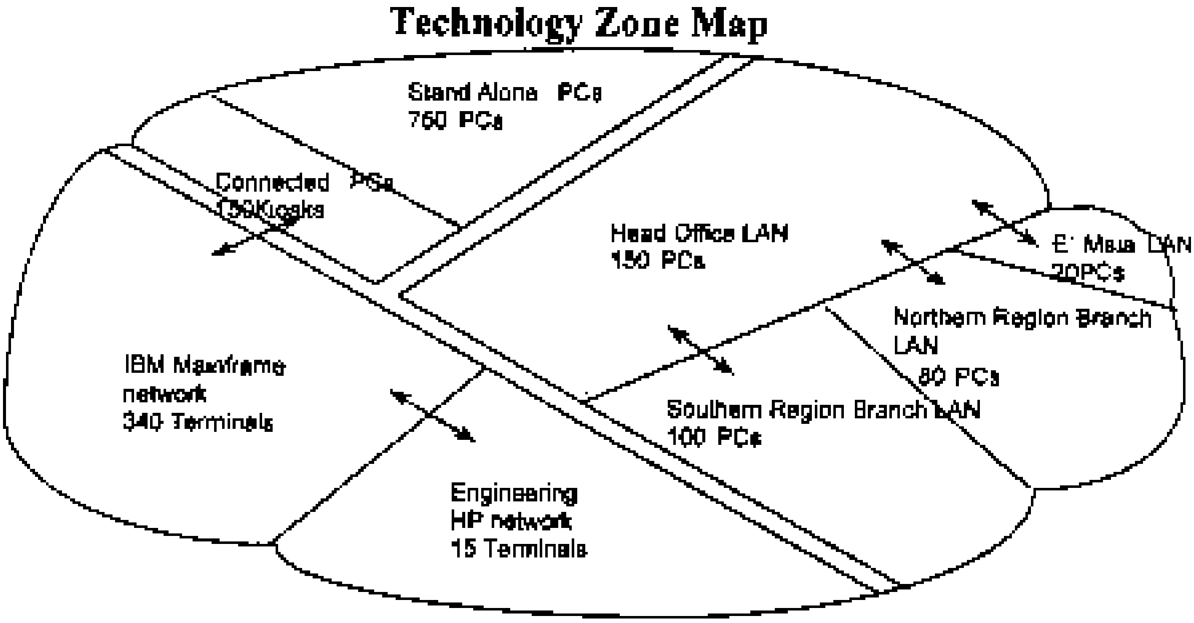
The Executive Summary is an important deliverable that will provide the Agency and other Government staff a clear overview of the Agency ISP. It will hopefully encourage Agency staff to read the detailed sections that comprise the ISP.

Provide a summary for the executive group that summarises the key findings and recommendations.

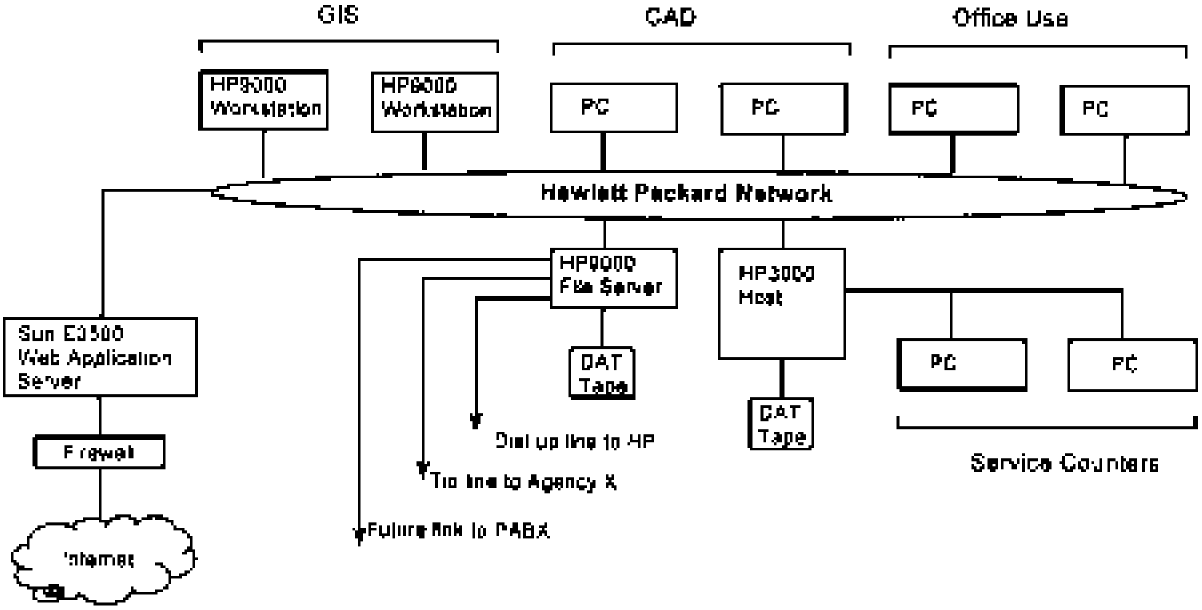
Sample Diagrams
Example 1 - Architecture Layer Diagram

Architecture Layer		**Host System**	**LAN Servers**	**Workstations**
Applications		For budgeting and other special core business functions, a suite of systems, custom designed to meet Agency requirements and interfaced where appropriate to the financial system, SAGA	For relatively routine business and corporate functions (HR, GL, AP, Library and Records Mgt etc) application packages preferably running on the LAN file servers	
Tools		Potentially an Economic Modelling Took	Standard MS Office Environment (Word, Excel, PowerPoint) E-mail (MS Mail)	
Development Environment	Tools	High Productivity Development Environment (Windows-4GL, Powerbuilder, Visual basic)	Standard User-Developer small systems development environment (MS Access)	
	DBMS	SQL based Relational Database (Oracle, Informix, Sybase)		
User Interface		Microsoft Environment (MS Windows or Work Groups for Windows)		
Access Security		Transparent Network and Database Security		
Network		Robust network operating system (Novell)		
Operating Systems		An open systems Operating System (UNIX, Windows NT)	MS DOS Windows NT	MS DOS
Hardware Platform		High Performance Host Processors(s) (HP, IBM, etc)	PCs - Pentium Firewall File Servers	Desk Top PCs Notebook PCs

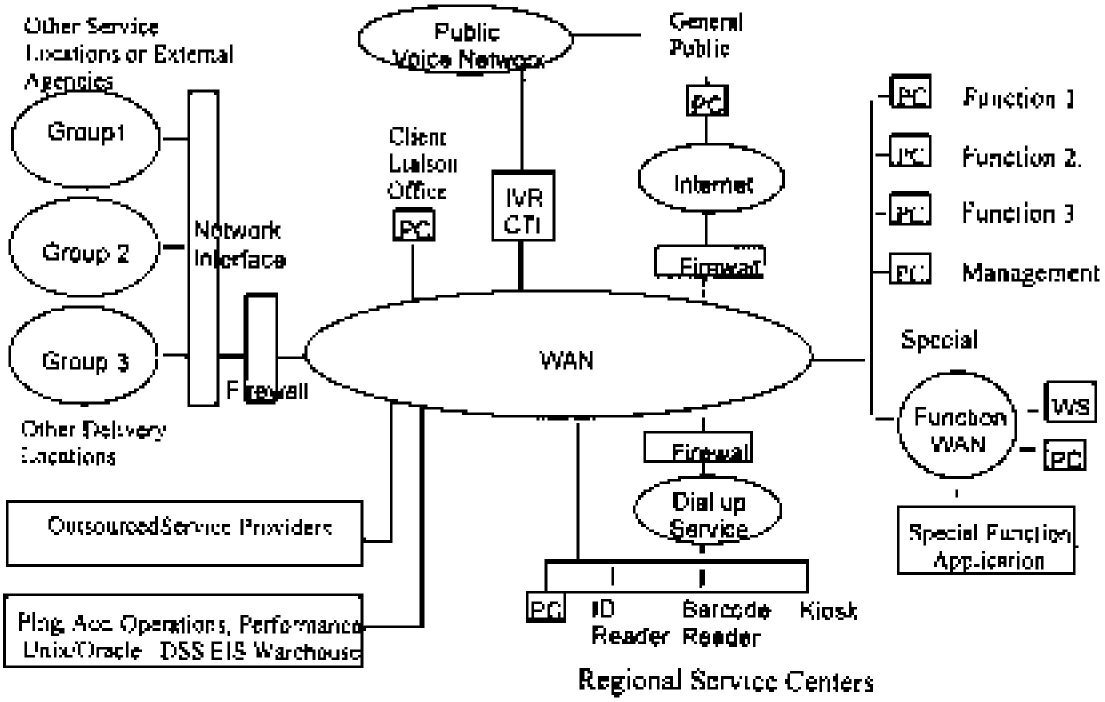
Example 2—Technology Zone Map



Example 3 – Network Diagram A



Example 4 – Network Diagram B



Appendix H

KERAJAAN MALAYSIA

PEKELILING AM BIL. 1 TAHUN 2001

MEKANISME PELAPORAN
INSIDEN KESELAMATAN TEKNOLOGI MAKLUMAT
DAN KOMUNIKASI (ICT)

JABATAN PERDANA MENTERI
MALAYSIA

Dikelilingkan Kepada:

Semua Ketua Setiausaha Kementerian
Semua Ketua Jabatan Persekutuan
Semua Ketua Pengurusan Badan Berkanun Persekutuan
Semua Y.B. Setiausaha Kerajaan Negeri
Semua Ketua Pengurusan Pihak Berkuasa Tempatan

JABATAN PERDANA MENTERI MALAYSIA
KOMPLEKS JABATAN PERDANA MENTERI
PUSAT PENTADBIRAN KERAJAAN PERSEKUTUAN
62502 PUTRAJAYA

Telefon: 603-8888 1957
Faks: 603-8888 3721

Rujukan Kami: PM (S) 10034 Jld. 8 (96)
Tarikh: 4 April 2001

Semua Ketua Setiausaha Kementerian
Semua Ketua Jabatan Persekutuan
Semua Ketua Pengurusan Badan Berkanun
Semua Y.B. Setiausaha Kerajaan Negeri
Semua Ketua Pengurusan Pihak Berkuasa Tempatan

PEKELILING AM BIL. 1 TAHUN 2001

MEKANISME PELAPORAN INSIDEN KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (ICT)

TUJUAN

Pekeliling ini bertujuan untuk menjelaskan mekanisme pelaporan insiden keselamatan teknologi maklumat dan komunikasi (ICT) bagi sektor awam.

LATAR BELAKANG

2. Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan yang dikeluarkan pada 1 Oktober 2000 melalui Pekeliling Am Bil. 3 Tahun 2000 telah merumuskan keperluan penguatkuasaan, kawalan dan langkah-langkah yang menyeluruh untuk melindungi aset ICT kerajaan bagi menjamin kesinambungan urusan kerajaan dengan meminimumkan kesan insiden keselamatan. Dengan itu satu mekanisme perlu diwujudkan untuk memantau perkara ini dan menentukan semua agensi sektor awam mematuhi dasar dan tatacara keselamatan ICT dan pada masa yang sama meningkatkan kesedaran mengenai keselamatan ICT di sektor awam.

INSIDEN KESELAMATAN

3. Insiden keselamatan bermaksud musibah *(adverse event)* yang berlaku ke atas sistem maklumat dan komunikasi (ICT) atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar dasar keselamatan ICT samada yang ditetapkan secara tersurat atau tersirat.

4. Kejadian insiden boleh berlaku dalam pelbagai keadaan. Insiden yang ketara dan sering berlaku di masa kini termasuk kejadian-kejadian berikut:

(a) Percubaan (sama ada gagal atau berjaya) untuk mencapai sistem atau data tanpa kebenaran *(probing)*;

(b) Serangan kod jahat *(malicious code)* seperti *virus, trojan horse, worms* dan sebagainya;

(c) Gangguan yang disengajakan *(unwanted disruption)* atau halangan pemberian perkhidmatan *(denial of service)*;

(d) Menggunakan sistem untuk pemprosesan data atau penyimpanan data tanpa kebenaran *(unauthorised access)*; dan

(e) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak.

5. Semua insiden keselamatan ICT yang berlaku di mana-mana agensi perlu dilaporkan kepada *Government Computer Emergency Response Team* (GCERT), satu pasukan khas yang ditempatkan di MAMPU bertanggungjawab menangani semua aduan mengenai insiden yang dilaporkan. Semua maklumat adalah SULIT, dengan itu tidak boleh didedahkan tanpa kebenaran agensi berkenaan.

TUJUAN PELAPORAN

6. Laporan mengenai insiden keselamatan ini adalah penting kepada GCERT untuk mendapat maklumat bagi membolehkannya menyediakan bantuan teknikal kepada agensi-agensi yang terlibat. Maklumat yang terkumpul juga boleh dijadikan panduan dalam menangani insiden yang sama yang berlaku di lokasi-lokasi yang lain. Ia juga boleh digunakan sebagai panduan bagi mengelak daripada kejadian yang sama berulang. Semua laporan yang diterima oleh GCERT akan dikumpulkan dalam pangkalan data dan maklumat ini merupakan input penting kepada perancangan strategik dan pemantauan mengenai keselamatan ICT di sektor awam. Dalam proses menyelesaikan sesuatu masalah, GCERT akan bekerjasama rapat dengan agensi terlibat dan pihak-pihak lain yang berkaitan. Interaksi seperti ini akan dapat meningkatkan pengetahuan di samping memupuk kerjasama dan hubungan baik di antara agensi.

TANGGUNGJAWAB *GOVERNMENT COMPUTER EMERGENCY RESPONSE TEAM* (GCERT)

Government Computer Emergency Response Team **(GCERT) di MAMPU adalah bertanggungjawab menangani semua laporan insiden keselamatan ICT yang melibatkan sektor awam. Secara amnya tugas GCERT adalah seperti berikut:**

(a) Menerima dan mengambil tindakan ke atas insiden keselamatan yang dilaporkan;

(b) Menyebarkan maklumat bagi membantu pengukuhan keselamatan ICT sektor awam dari semasa ke semasa;

(c) Menyediakan khidmat nasihat kepada agensi-agensi dalam mengesan, mengenalpasti dan menangani sesuatu insiden keselamatan; dan

(d) Menjadi penyelaras dengan pihak-pihak yang terlibat seperti *Malaysian Computer Emergency Response Team* (MyCERT), pembekal, *Internet Service Provider* (ISP) dan agensi-agensi penguatkuasa.

KEUTAMAAN TINDAKAN

8. Tindakan ke atas insiden yang dilaporkan akan dibuat berasaskan keparahan sesuatu insiden. Secara amnya keutamaan akan ditentukan seperti berikut:

Keutamaan 1:

Aktiviti yang berkemungkinan mengancam nyawa atau keselamatan negara.

Keutamaan 2 :

(a) Pencerobohan atau percubaan menceroboh melalui infrastruktur internet ke atas:

i. *Domain Name Servers* (DNS)

ii. *Network Access Points* (NAPs)

iii. Pusat-pusat pangkalan data utama

(b) Halangan pemberian perkhidmatan yang meluas *(Distributed Denial of Service)*;

(c) Serangan atau pendedahan bahaya terbaru *(new vulnerabilities)*; atau

(d) Jenis-jenis insiden lain seperti:

i. Pencerobohan melalui pemalsuan identiti

ii. Pengubahsuaian laman web, perisian, atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan pihak yang berkenaan; atau

iii. Gangguan sistem untuk pemprosesan data atau penyimpanan data tanpa kebenaran.

TANGGUNGJAWAB AGENSI PELAPOR

9. Agensi yang mengalami insiden keselamatan adalah dimestikan melapor setiap insiden kepada GCERT. Setiap agensi perlu menyediakan prosidur operasi atau *Standard Operating Procedure* (SOP) berdasarkan infrastruktur ICT masing-masing supaya setiap insiden yang berlaku dapat ditangani dengan segera dan sistematik. Tugas-tugas ini diletakkan di bawah tanggungjawab Ketua Pegawai Makumat (CIO) dan Pegawai Keselamatan ICT (ICTSO).

10. Tugas CIO dalam aspek ini adalah seperti berikut:

(a) Menguruskan tindakan ke atas insiden yang berlaku sehingga keadaan pulih;

(b) Mengaktifkan *Business Resumption Plan* (BRP) jika perlu; dan

(c) Menentukan samada insiden ini perlu dilaporkan kepada agensi penguatkuasaan undang-undang/keselamatan.

11. Secara khusus tugas ICTSO dalam menangani insiden keselamatan ICT pula adalah seperti berikut:

(a) Menentukan tahap keutamaan insiden;

(b) Melaporkan insiden kepada GCERT; dan

(c) Mengambil langkah pemulihan awal.

PROSES PELAPORAN

12. Proses pelaporan dijelaskan di lampiran A. Lampiran A1 menunjukkan hubungan antara agensi dan entiti yang terlibat dalam proses pelaporan manakala Lampiran A2 merupakan aliran kerja terperinci bagi proses pelaporan insiden keselamatan ICT sektor awam.

KAEDAH PELAPORAN

13. Laporan boleh dibuat menggunakan kaedah-kaedah berikut:-

(a) Mel Elektronik (E-mel) :-

Alamat e-mel : gcert@mampu.gov.my

(b) Borang Pelaporan Insiden :-

Boleh diperolehi di laman : http://gcert.mampu.gov.my

(c) Telefon *Hotline*

Nombor tel. : 03-88883150

(d) Faks

Nombor faksimili : 03-88883286

(e) Bagi agensi yang mempunyai kemudahan aplikasi PGP (*Pretty Good Practice*) sila gunakan *PGP Public Key* seperti di bawah untuk *encrypt* laporan yang akan dihantar kepada GCERT. *Key* tersebut juga boleh didapati di laman web GCERT:- http://gcert.mampu.gov.my

KHIDMAT NASIHAT

14. Sebarang kemusykilan yang timbul berkaitan dengan Surat Pekeliling ini hendaklah dirujuk kepada GCERT, seperti di bawah:

Government Computer Emergency Response Team (GCERT)
Bahagian Keselamatan ICT, MAMPU
Aras 5, Blok B1, Parcel B
Kompleks Jabatan Perdana Menteri
Pusat Pentadbiran Kerajaan Persekutuan
62502 PUTRAJAYA

No. *Hotline* : 03-88883150
No. Faksimili : 03-88883286
E-mel : gcert@mampu.gov.my

15. Khidmat GCERT boleh diperolehi setiap hari bekerja mulai pukul 8.15 pagi hingga 4.45 petang. Sekiranya agensi menghadapi insiden yang kritikal, iaitu insiden di bawah Keutamaan 1, di perenggan 8, GCERT boleh dihubungi serta merta dan jika ia berlaku di luar masa pejabat, pegawai yang boleh dihubungi adalah seperti berikut:

(a) Bahagian Keselamatan ICT

(i) Pengarah : 03-88882250

(ii) Timbalan Pengarah : 03-88882581

(b) Pasukan GCERT:

(i) Pengurus : 03-88882273

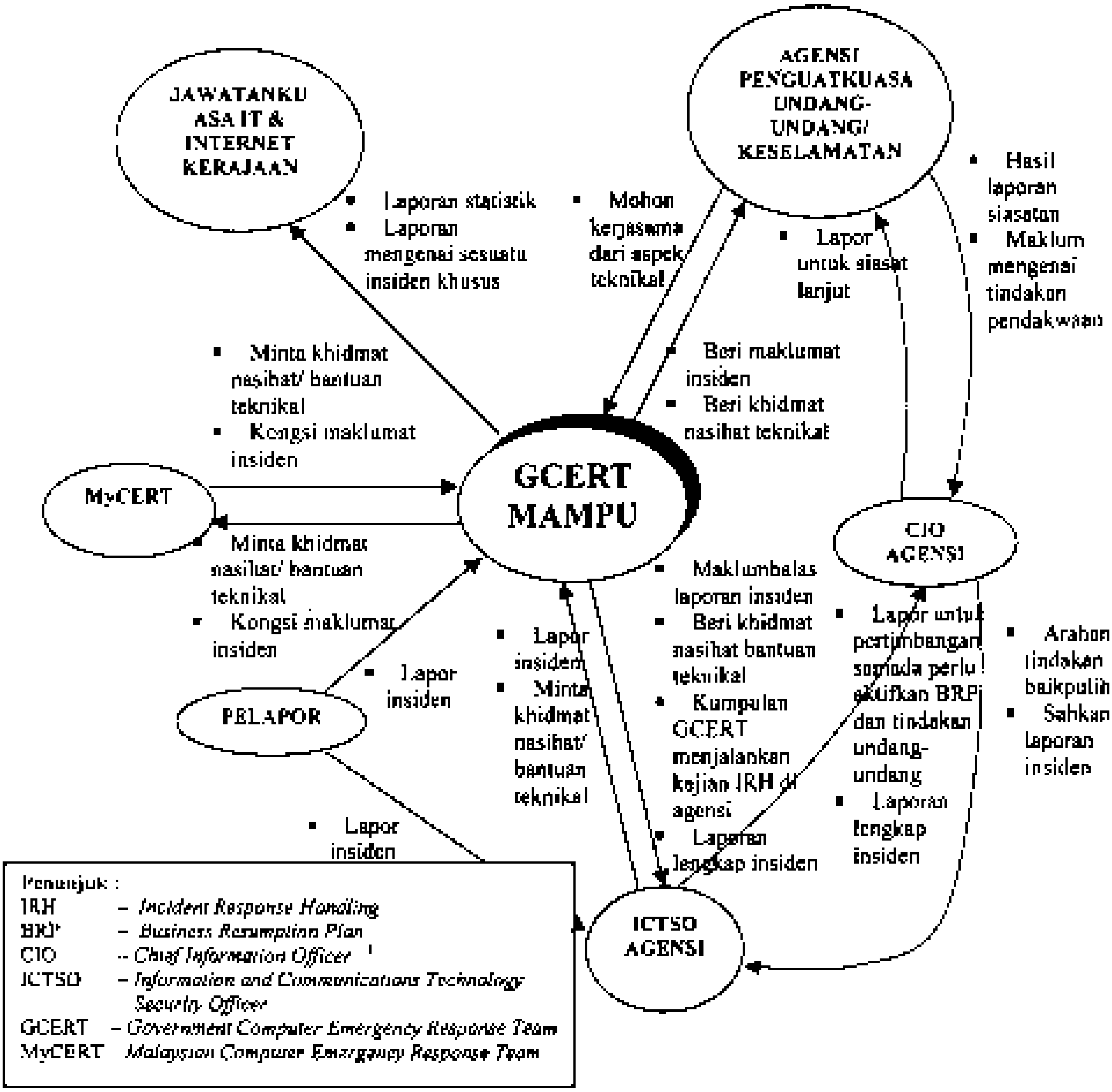
(ii) Pegawai : 03-88882587

TARIKH KUATKUASA

16. Surat arahan ini berkuatkuasa mulai tarikh surat ini dikeluarkan.

(TAN SRI SAMSUDIN BIN OSMAN)
Ketua Setiausaha Negara

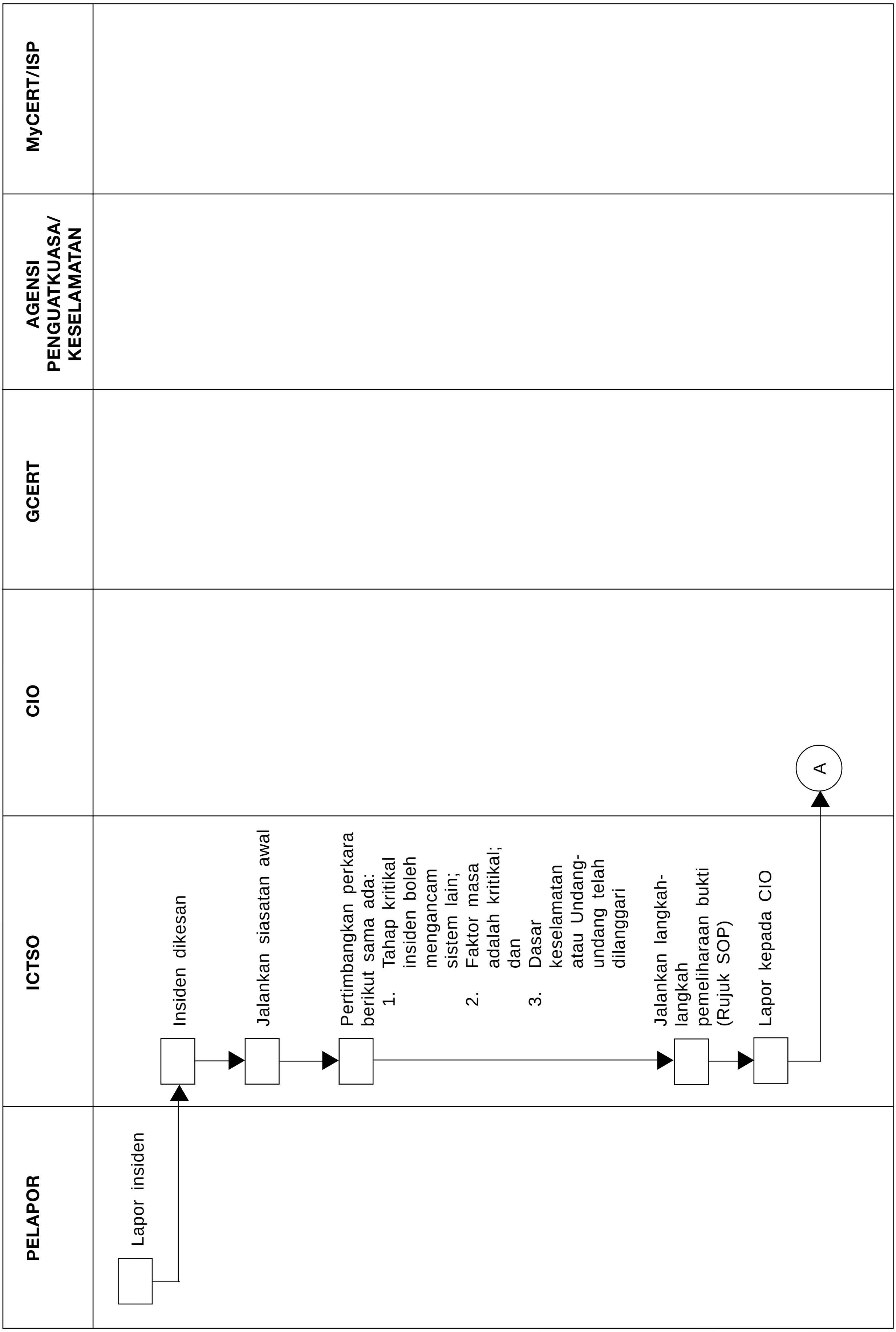
LAMPIRAN A

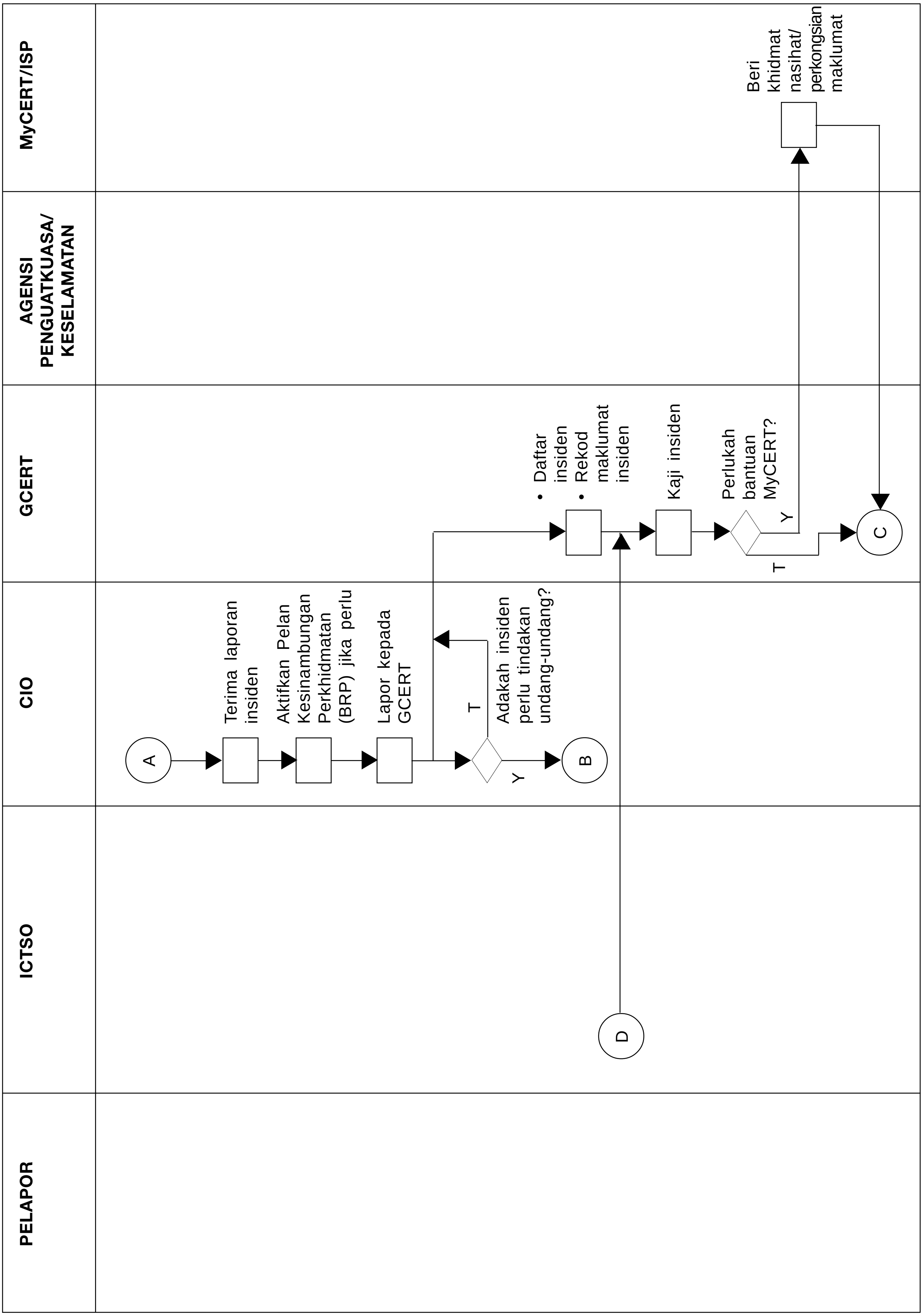

JAWATANKUASA IT & INTERNET KERAJAAN
AGENSI PENGUATKUASA UNDANG-UNDANG/ KESELAMATAN
GCERT MAMPU
MyCERT
CIO AGENSI
PELAPOR
ICTSO AGENSI
▪ Laporan statistik
▪ Laporan mengenai sesuatu insiden khusus
▪ Mohon kerjasama dari aspek teknikal
▪ Lapor untuk siasat lanjut
▪ Hasil laporan siasatan
▪ Maklum mengenai tindakan pendakwaan
▪ Minta khidmat nasihat/ bantuan teknikal
▪ Kongsi maklumat insiden
▪ Beri maklumat insiden
▪ Beri khidmat nasihat teknikal
▪ Minta khidmat nasihat/ bantuan teknikal
▪ Kongsi maklumat insiden
▪ Lapor insiden
▪ Lapor insiden
▪ Minta khidmat nasihat/ bantuan teknikal
▪ Maklumbalas laporan insiden
▪ Beri khidmat nasihat bantuan teknikal
▪ Kumpulan GCERT menjalankan kajian IRH di agensi
▪ Laporan lengkap insiden
▪ Lapor untuk pertimbangan sekiranya perlu aktifkan BRP dan tindakan undang-undang
▪ Laporan lengkap insiden
▪ Arahan tindakan baikpulih
▪ Sahkan laporan insiden
▪ Lapor insiden

Penunjuk :
IRH – *Incident Response Handling*
BRP – *Business Resumption Plan*
CIO – *Chief Information Officer*
ICTSO – *Information and Communications Technology Security Officer*
GCERT – *Government Computer Emergency Response Team*
MyCERT *Malaysian Computer Emergency Response Team*

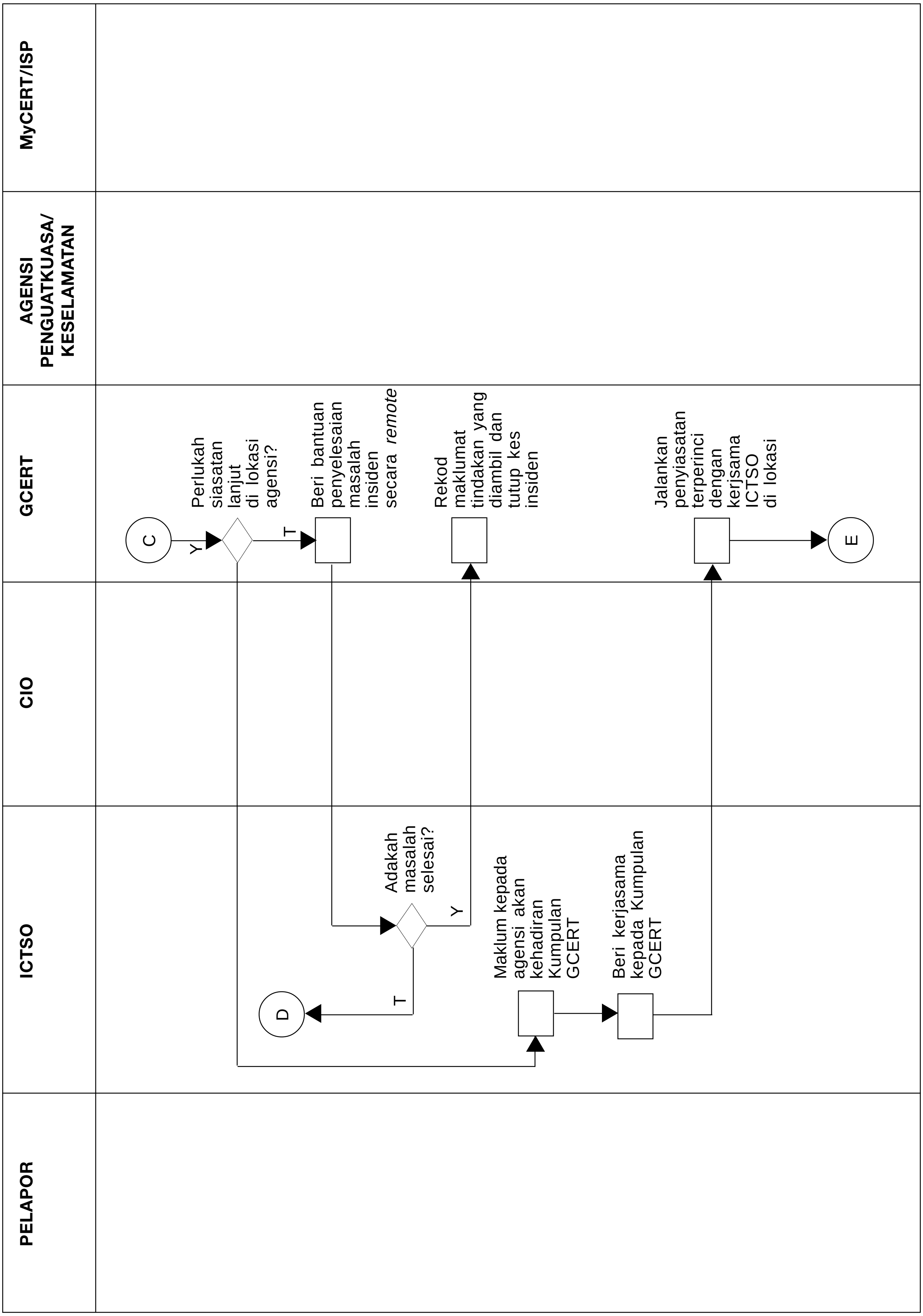
Rajah 1: Hubungan Entiti dalam Proses Kerja Pelaporan Insiden Keselamatan ICT

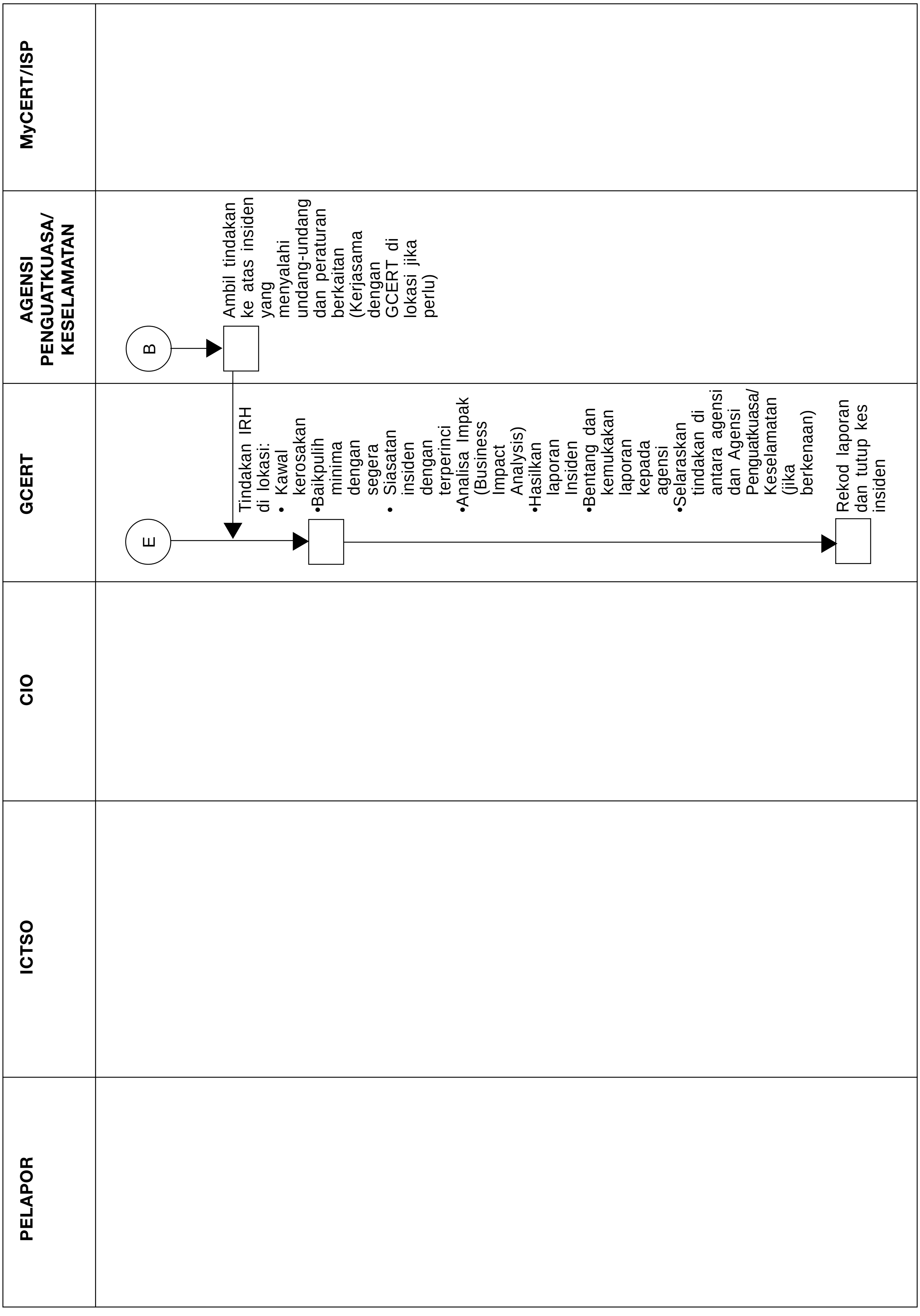
5.2 Rajah 2 : Jadual Terperinci Bagi Proses Kerja Pelaporan Insiden Keselamatan ICT Agensi yang terlibat


PELAPOR
ICTSO
CIO
GCERT
AGENSI PENGUATKUASA/ KESELAMATAN
MyCERT/ISP
Lapor insiden
Insiden dikesan
Jalankan siasatan awal
Pertimbangkan perkara berikut sama ada:
1. Tahap kritikal insiden boleh mengancam sistem lain;
2. Faktor masa adalah kritikal; dan
3. Dasar keselamatan atau Undang-undang telah dilanggari
Jalankan langkah-langkah pemeliharaan bukti (Rujuk SOP)
Lapor kepada CIO
A


MyCERT/ISP
AGENSI PENGUATKUASA/ KESELAMATAN
GCERT
CIO
ICTSO
PELAPOR
A
Terima laporan insiden
Aktifkan Pelan Kesinambungan Perkhidmatan (BRP) jika perlu
Lapor kepada GCERT
Adakah insiden perlu tindakan undang-undang?
T
Y
B
• Daftar insiden
• Rekod maklumat insiden
Kaji insiden
Perlukah bantuan MyCERT?
Y
T
C
Beri khidmat nasihat/ perkongsian maklumat
D

Copyright MAMPU


MyCERT/ISP
AGENSI PENGUATKUASA/ KESELAMATAN
GCERT
CIO
ICTSO
PELAPOR
C
Y
Perlukah siasatan lanjut di lokasi agensi?
T
Beri bantuan penyelesaian masalah insiden secara *remote*
Rekod maklumat tindakan yang diambil dan tutup kes insiden
Jalankan penyiasatan terperinci dengan kerjasama ICTSO di lokasi
E
Adakah masalah selesai?
Y
T
D
Maklum kepada agensi akan kehadiran Kumpulan GCERT
Beri kerjasama kepada Kumpulan GCERT


MyCERT/ISP
AGENSI PENGUATKUASA/ KESELAMATAN
GCERT
CIO
ICTSO
PELAPOR
B
Ambil tindakan ke atas insiden yang menyalahi undang-undang dan peraturan berkaitan (Kerjasama dengan GCERT di lokasi jika perlu)
E
Tindakan IRH di lokasi:
• Kawal kerosakan
•Baikpulih minima dengan segera
• Siasatan insiden dengan terperinci
•Analisa Impak (Business Impact Analysis)
•Hasilkan laporan Insiden
•Bentang dan kemukakan laporan kepada agensi
•Selaraskan tindakan di antara agensi dan Agensi Penguatkuasa/ Keselamatan (jika berkenaan)
Rekod laporan dan tutup kes insiden

Appendix I

A SAMPLE HELP DESK REPORTING FORM

Name : ______________________________

Location : ______________________________

Date/Time : ______________________________

Description of Problem : ______________________________

Date of Occurrence : ______________________________

Level : Less Critical □ Medium □ Critical □

Action : ______________________________

Action Taken By (Date/Time) : ______________________________

Appendix J

A SAMPLE EMPLOYEE AWARENESS FORM

EMPLOYEE AWARENESS FORM

Employee Awareness Form is to find out about the security awareness of the staff.

Please write your details below:

Organisation :

Department :

Name and Position :

Date :

Copyright MAMPU

Record your assessment by checking at the appropriate columns.

Security Element	Yes	No
Physical Security Is your computing equipment properly secured? Is your computer inside an area which is not easily accessible to someone who might steal it or its components? Is your office properly secured when no one is there?		
Virus and Threat Protection Do you have the latest anti-virus software for your computer? Do you usually scan to check all floppies for viruses before you use them? Do you use different disks between your home and office computers? Does your organisation scan servers and desktops periodically for security vulnerabilities?		
Operating Systems Are the operating systems you use updated with current security “patches’? Do you feel that the file permissions are verified and set properly on your servers?		
Application Software Are your common applications configured for security? Does the staff have the appropriate level of access to applications based on their current responsibilities? Is application access promptly removed for employees who have left the department?		
Confidentiality of Sensitive Data Do you work with sensitive information such as financial data or personnel records? Are you exercising your responsibility to protect sensitive data under your control? Are you aware that sensitive data or memo send via e-mail should be encrypted?		

Copyright MAMPU

Passwords Have you changed your password in the last one-month? Do you use different passwords for office administrative work as you do for other activities such as Web surfing? Do you keep your password secret from your friends, co-workers or boss?		
Disaster Recovery Does your organisation have a disaster recovery plan? Would you be able to continue working without your computer? Do you know what to do and whom to contact if you have an ICT computer security incident?		
Data Back-up and Restoration Do you back-up all important files or records? Have you back-up your computer files this week? Is your back-up data stored in a secured site?		
Encryption Do you know what encryption is? Are Official Secret data in your organisation encrypted? Do you encrypt Official Secret information stored digitally?		
Security Awareness and Education Are you aware of your organisation or departmental ICT security policies, guidelines or procedures to protect information? Do you always use licensed software? Do you register shareware in your office? Have you had any training on ICT computer security?		

Appendix K

A SAMPLE EMPLOYEE SECURITY CHECKLIST

	Yes	No
Is there an individual or department responsible for computer related security?	□	□
Are applicant references and background fully checked prior to employment?	□	□
Do relevant employees sign the agreement?	□	□
Are all new personnel advised on internal security practices?	□	□
Is there a formal manual defining the organisation's security standards and procedures?	□	□
Is this manual mandatory reading for new personnel?	□	□
Are changes in security practices incorporated in the manual and disseminated to the staff?	□	□
Is there an on-going programme of computer security education for all user personnel?	□	□
Is the programme kept current?	□	□
Is there an individual or a committee responsible for monitoring compliance with security standards and procedures?	□	□
Is a security check carried out for contract and temporary personnel?	□	□
Are the security arrangements for temporary personnel the same as those of full time employees?	□	□
Are identifications used to identify personnel?	□	□
Do the identifications indicate the level of employment security?	□	□
Are all personnel engaged in confidential or other sensitive work requested to leave immediately on resignation or dismissal?	□	□

Appendix L

DISASTER RECOVERY AND CONTINGENCY PLANNING CHECKLIST FOR ICT SYSTEMS

I. GETTING READY

□ **A.** Obtain written commitment from top management of support for contingency planning objectives.

□ **B.** Assemble the contingency planning team to include one or more permanent members from:

1. Computer support staff
2. Operational or unit managers
3. Facilities management
4. Department Safety Committee
5. ICTSO

□ **C.** Provide for the planning committee to include participation on an “as needed” basis from the following departments:

1. Internal Audit (compliance)
2. Police (coordination)
3. Information & Communications Technology (ICT)
4. Others as required.

□ **D.** Define the responsibility of planning committee members. Appoint;

1. Moderator to facilitate planning meetings
2. Secretary to take and prepare meeting notes and agenda’s
3. Administrator to aggregate meeting materials

II. GATHERING NECESSARY INFORMATION - RISK ASSESSMENT

□ **A.** Prepare a written description of the mission - critical functions of the Department and Units.

□ **B.** Identify the areas impacted by an emergency:

1. Functional Operation of the Department
2. Service to Clients/ Staff
3. Obligations to Vendors/ Suppliers/ Agencies
4. Relations with Other Departments
5. Department Credibility
6. Other Departmental Impacts

Copyright MAMPU

□ **C.** Define and establish estimated potential losses and liability to the department due to lost or delayed functions, in order of severity of the emergency:

Severity	Amount or range (RM)	Duration
1. Catastrophic	______________________	_______
2. Major	______________________	_______
3. Serious	______________________	_______
4. Limited	______________________	_______

□ **D.** Determine which critical department functions depend on ICT systems. List critical functions with the associated ICT system(s). Contingency planning for critical functions beyond their information systems components should be referred to the department recovery planning effort.

□ **E.** Establish the vulnerability of ICT systems by examining possible consequences and frequency of specific emergencies.

Specific Emergencies

1. Earthquake
2. Fire
3. Flood
4. Landslide
5. Bomb/ Explosion
6. Sabotage
7. Power Failure/ surge
8. Other?

Possible Consequences

1. Prohibited Access
2. Disrupted Power
3. Power Outage
4. Water Damage
5. Smoke Damage
6. Chemical Damage
7. Structural Damage
8. Communication loss
9. Other?

□ **F.** Using the information in **A through E** make a prioritized list of mission critical ICT system functions for restoration in an emergency.

III. GATHERING NECESSARY INFORMATION - RESOURCE ASSESSMENT

□ **A.** Survey the systems and data which are critical to the Department's functions. Develop flow charts of the results. Verify flow diagrams with appropriate system administrator. The survey should ascertain:

1. Source of all data used in the system
2. Nature of information or report
3. Frequency of need for data
4. How the data is obtained, paper, e-mail, remote access download, tape or disk.
5. Who in department receives or retrieves data.

6. Who on the department do you speak to about access to the data? Will they be available in an emergency?
7. What is the impact if this data is not available
8. Hardware/ OS software
9. Network.
10. Applications.

□ **B.** Determine if the current backup plan is adequate for the completed risk assessment and includes the following features:

1. Routine periodic backups,
2. Clear backup “strategy” (full vs. incremental backups, frequency, etc.),
3. Off-site storage and retrieval procedures,
4. Alternate processing site (hot, warm, or cold site)

□ **C.** Complete a resource inventory in each of the following areas (items that might have to be replaced):

1. Equipment
   a. Computer hardware
   b. Network hardware
   c. Other equipment
2. Documentation
   a. Procedure manuals/ handbooks
   b. Software
   c. Accounting procedures
   d. Communication documentation
3. Others

□ **D.** Define the responsibilities of emergency response team(s).

□ **E.** Complete staff responsibility chart for emergency response.

1. Disaster evaluation team (management level)
2. Interim operations team
3. Recovery team

IV. INTEGRATION WITH DEPARTMENT RESPONSE AND RECOVERY PLANNING

□ **A.** Specify who is authorized to declare a disaster and activate the information systems emergency Plan.

□ **B.** Define the department's immediate response actions by referring to the Department Safety Plan for evacuation and notification of staff.

1. Accounting for staff and others in the building.
2. Meeting location of disaster evaluation team.
3. Reaching staff needed for emergency response.
   a. List of home telephone numbers
   b. Cellular phone

□ **C.** The Department Recovery Plan should define "manual" processes that can be used until ICT resources are recovered. This need for parallel paper process is beyond the planning scope of information system group. It needs to be defined by a department administrative recovery team. This plan should:

1. Stock the required forms.
2. Pre-assign batch numbers, queue numbers, work order numbers, service request numbers, etc.
3. Document procedures to merge the manually tracked data with the information on the system once it is restored.
4. Prescribe how the impact of changes in procedures will be clear to customers, vendors, etc.

V. INTERIM OPERATION PLAN - PREARRANGED AGREEMENTS FOR RESOURCE REPLACEMENT

□ **A.** Possibilities for alternate site:

1. Other department with similar facilities
2. Other department in the immediate geographical area
3. Computer manufacturer's facilities (or other suggestions from them)
4. Service bureaus in the immediate area

□ **B.** Considerations for alternate site selection:

1. Building type
2. Floor capacity - space and load
3. Raised flooring
4. Electric circuits/ capacity/ special connectors
5. Air conditioning and humidity control
6. Chilled water
7. Fire protection and suppression
8. Security - personnel
9. Security - physical
10. Security - data
11. Communications
    a. Telephones.
    b. Network between departmental systems and access to other data.
    c. Physical access to systems with critical data which are not accessible remotely.

□ **C.** Back-up agreements:

1. Written guarantee or contract with other companies.
2. Reciprocal agreements
3. Service bureau commitments
4. Vendor commitments

□ **D.** Alternate hardware:

1. Computer and components
   a. CPU model
   b. Memory
   c. Operating system
   d. Options
   e. Peripherals
2. Network equipment and wiring
3. Terminals
4. Off-line equipment
5. Furniture
6. Office machines (including phones, fax, etc.)

□ **E.** Supplies:

1. Paper
2. Forms
3. Disks
4. Tapes
   a. Reel
   b. Cartridge (type)

□ **F.** Off-site moving plans:

1. Transportation of staff
2. Transportation of data and supplies
3. Staff phone list
4. Other ______

VI. TEST, EVALUATE AND UPDATE THE PLAN

□ **A.** Specify periodic testing of the contingency plan to assure processing compatibility:

1. Frequency
2. Scope
3. Test data
4. Test evaluation team

□ **B.** Periodically review and update of emergency response documentation:

1. Staff responsibility charts
2. Staff telephone numbers
3. Vendors
4. Software license agreements
5. Alternate site agreements
6. Inventory of computer hardware and software
7. Interim operations procedures

□ **C.** Periodically review and drill emergency response and recovery teams:

1. Tabletop exercise to test documentation and communication in controlled environment.
2. Functional exercise to test documentation, communication and procedures in controlled environment.
3. Field exercise to test documentation, communication, procedures and logistics in a simulated “real” environment.

VII. RECOVERY AND RESTORATION

□ **A.** Permanent site preparation:

1. Building
2. Floor capacity - space and load
3. Raised flooring
4. Electric circuits/ capacity/ special connectors
5. Air conditioning and humidity control
6. Chilled water
7. Fire protection and suppression
8. Security - staff
9. Security - physical
10. Security - data
11. Communications
    a. Telephones
    b. Network between departmental systems and access to other data
    c. Physical access to systems with critical data which are not accessible remotely.

□ **B.** Procurement of hardware:

1. Acquisition
2. Computer and components
    a. CPU model
    b. Memory
    c. Operating system
    d. Options
    e. Peripherals

3. Network equipment and wiring
4. Terminals
5. Off-line equipment
6. Furniture
7. Office machines (including phones, fax, etc.)

□ **C.** Supplies:

1. Paper
2. Forms
3. Disks
4. Tapes
    a. Reel
    b. Cartridge (type)

□ **D.** Parallel operations plans.

□ **E.** Migration plan

□ **F.** Procedures to close down the interim operation