

Acknowledgement

The Government of Malaysia is committed towards modernising its administrative machinery and enhancing its service delivery mechanisms. The process of ensuring an efficient and effective public sector is being driven by the enabling capabilities of information and communications technology (ICT). The resultant widespread adoption of ICT systems by the public sector has meant that more and more Government agencies are moving towards the paperless work environment where ICT systems have become indispensable for the provision of Government services to citizens.

The expansion of ICT systems within the public sector has in turn led to a significant increase in the number of public sector information repositories and other ICT-based installations and assets. The security of these ICT installations and assets are exposed to the vulnerability of open and networked electronic systems. As such agencies now face the additional responsibility of securing ICT-based Government information and systems as well as ensuring that they are available to authorised users.

The Malaysian Public Sector ICT Management Security Handbook (**MyMIS**) is intended as a reference and guide for public sector personnel in managing security in all public sector ICT installations. **MyMIS** serves to complement the ICT security measures taken earlier by the Government by way of *Pekeliling Am Bil. 3 Tahun 2000* entitled '*Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan*' (Government Information and Communications Technology Security Policy Framework) and *Surat Pekeliling Am Bil.1 Tahun 2001* entitled '*Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)*' (Information and Communications Technology (ICT) Security Incident Reporting Mechanism).

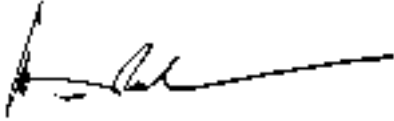
While every effort has been made to address all possible ICT security situations in the handbook, there will of course be instances during normal ICT operations where the incidents encountered may not be sufficiently covered in this handbook. In the event of such cases, the best practice available for the relevant situation should be followed.

Needless to say, the **MyMIS** handbook is the product of close collaboration between MAMPU and various other Government agencies. Their contributions have certainly helped sustain the momentum during periods of waning energy in the course of completing this handbook. MAMPU would therefore like to place on record its appreciation to the following agencies:

- National Security Division, *Prime Minister's Department (Bahagian Keselamatan Negara, Jabatan Perdana Menteri)*
- Office of the Chief Government Security Officer, *Prime Minister's Department (Pejabat Ketua Pegawai Keselamatan Kerajaan, Jabatan Perdana Menteri)*
- Ministry of Energy, Communications and Multimedia (*Kementerian Tenaga, Komunikasi dan Multimedia*)
- Ministry of Defence (*Kementerian Pertahanan*)
- National Institute of Public Administration (INTAN)
- Universiti Teknologi Malaysia
- Universiti Kebangsaan Malaysia
- Universiti Putra Malaysia
- Universiti Malaya
- Bank Negara Malaysia
- GITN Sdn. Berhad
- MIMOS Berhad
- SIRIM Berhad

I wish to also express my appreciation to Y. Bhg. Tan Sri Samsudin Osman, Chief Secretary to the Government of Malaysia, for entrusting MAMPU with the task of preparing and publishing this handbook.

Finally, I thank my officers and staff in MAMPU, in particular those in the ICT Security Division who were actively involved in the entire process of conceptualising, drafting, reviewing and publishing this handbook.



DATUK DR. MUHAMMAD RAIS BIN ABDUL KARIM
Director-General
Malaysian Administrative Modernisation and Management
Planning Unit (MAMPU)
Prime Minister's Department, Malaysia
January 2002



Chief Secretary to the Government

The Internet-driven global digital revolution and the explosive growth of computer networks and systems have resulted in the extensive use of information and communications technology (ICT) for gathering, maintaining and transmitting information and data. Electronic connectivity in the work place has meant that the security of ICT systems and the information residing in them can no longer be provided through conventional means. The increasing incidence of hacking, virus attacks and other forms of electronic trespass have necessitated the need for securing the new electronic work environment. The public sector is not insulated from the prevailing dangers of the digital world. For that matter, considering the scope of its functions, services and transactions as well as the complexities of its inter-relationships with all components of society, the public sector has to seriously address all concerns relating to ICT security.

For the Malaysian public sector, ICT security is critical to the objective of implementing Electronic Government and expanding the use of ICT in the delivery of Government services as well as in enhancing the internal operations of public sector agencies. In this regard, the Government has already issued a broad policy guideline on the underlying principles of ICT security, the responsibility of safeguarding Government information and the need for awareness about threats to the integrity of information and ICT assets. In addition, guidelines on the mechanism for reporting ICT security incidents were also issued to assist agencies in handling ICT security incidents in the public sector.

This Malaysian Public Sector Management of Information and Communications Technology Security Handbook (**MyMIS**) serves to complement the overall approach towards safeguarding ICT security in the public sector. It provides a comprehensive set of practical instructions to public sector agencies in managing and securing information and other ICT assets in their respective organisations. **MyMIS** will ensure that due attention is given to the entire range of activities related to the operations of a particular ICT-based facility, infrastructure, system or application. In this way, public sector agencies can be confident of the integrity, authenticity and availability of their services and outputs. As such, while satisfying the service requirements of customers at the individual level, public sector agencies can ensure privacy and confidentiality in all ICT-based transactions while safeguarding against any breach of national security.

I am confident that **MyMIS** will prove to be an extremely useful source of reference for all public sector agencies in implementing an effective ICT security management paradigm in their respective organisations. While we understand that there cannot be a guarantee of absolute security within internetworked electronic work environments, adherence to guidelines as prescribed by **MyMIS** will go a long way in mitigating much of the risks that ICT-based systems are exposed to. Public sector agencies should therefore ensure that the relevant levels of management within their organisations are informed and understand the contents of the handbook which is meant to serve as the standard guide for all ICT security management decisions and tasks. Finally, I wish to congratulate MAMPU and all others involved in coming out with this handbook.

TAN SRI SAMSUDIN OSMAN
Chief Secretary to the Government, Malaysia
January 2002

Table of Contents

	Page
Acknowledgement	i
Chief Secretary to the Government	iii
Table of Contents	v
List of Tables	xiii
List of Figures	xiv
List of Appendices	xv
Chapter 1 INTRODUCTION	1 - 1
1.1 General	1 - 1
1.2 Standards Framework	1 - 2
1.3 Handbook Coverage	1 - 3
1.4 Audience	1 - 4
Chapter 2 MANAGEMENT SAFEGUARDS	2 - 1
2.1 Public Sector ICT Security Policy	2 - 1
2.1.1 Central Level	2 - 2
2.1.2 Ministry/State Level	2 - 2
2.1.3 Departmental Level	2 - 3
2.2 Public Sector ICT Security Programme Management	2 - 3
2.2.1 Central Public Sector ICT Security Programme Management	2 - 4
2.2.2 Operating Level Public Sector ICT Security Programme Management	2 - 4
2.3 Public Sector ICT Security Risk Management	2 - 5
2.3.1 Formation of Risk Management Committee	2 - 5
2.3.2 Identification of Risks and Threats	2 - 6
2.3.3 Evaluation of Risks and Threats	2 - 6
2.3.4 Identification of Necessary Safeguards	2 - 7
2.3.5 Managing Residual Risks	2 - 8
2.3.6 Implementing Safeguards and Monitoring Effectiveness	2 - 8
2.3.7 Uncertainty Analysis	2 - 8

	Page	
2.4	Incorporating Public Sector ICT Security into the System Life Cycle	2 - 9
2.4.1	Benefits of Integrating Public Sector ICT Security in the System Life Cycle	2 - 9
2.4.2	The ICT System Life Cycle Phases	2 - 9
2.5	Public Sector ICT Security Assurance	2 - 11
2.5.1	Design and Implementation Assurance	2 - 11
2.5.1.1	Testing and Certification	2 - 11
2.5.1.2	Conformance Testing	2 - 12
2.5.1.3	Use of Reliable Architectures	2 - 12
2.5.1.4	Ease of Safe Use	2 - 12
2.5.1.5	Evaluation and Reviews	2 - 12
2.5.1.6	Assurance Documentation	2 - 13
2.5.1.7	Certification of Product to Operate in Similar Situation	2 - 13
2.5.1.8	Self-Certification	2 - 13
2.5.1.9	Warranties and Liabilities	2 - 13
2.5.1.10	Distribution Assurance	2 - 14
2.5.2	Operational Assurance	2 - 14
2.5.2.1	Audit Methods and Tools	2 - 14
2.5.2.2	Monitoring Methods and Tools	2 - 16
2.6	Operational Assurance Issues	2 - 18
Chapter 3	BASIC OPERATIONS	3 - 1
3.1	Information Classification	3 - 1
3.2	Roles and Responsibilities	3 - 2
3.2.1	Head of Department	3 - 2
3.2.2	Chief Information Officer	3 - 3
3.2.3	Computer Manager	3 - 3
3.2.4	ICT Security Officer	3 - 4
3.2.5	System Administrators	3 - 5
3.2.6	Help Desk	3 - 5
3.2.7	Users	3 - 5
3.2.8	Vendors, Contractors and External Service Providers	3 - 6

	Page
3.3 Human Factors	3 - 6
3.3.1 Personnel Security	3 - 7
3.3.1.1 Confidentiality Agreement	3 - 7
3.3.1.2 Personnel Screening	3 - 7
3.3.2 Awareness	3 - 7
3.3.3 Problem Employees	3 - 7
3.3.4 Former Employees	3 - 7
3.4 Electronic Facilities	3 - 8
3.4.1 Telecommuting	3 - 8
3.4.2 Voice, Telephone and Related Equipment	3 - 8
3.4.2.1 Access to Voice Mail system	3 - 9
3.4.2.2 Private Branch Exchange	3 - 9
3.4.2.3 Spoken Word	3 - 9
3.4.2.4 Intercept	3 - 10
3.4.2.5 Casual Viewing	3 - 10
3.4.2.6 Output Distribution Schemes	3 - 10
3.4.2.7 Destruction	3 - 10
3.4.2.8 Clock Synchronization	3 - 10
3.4.3 Facsimile	3 - 10
3.4.3.1 Modification	3 - 11
3.4.3.2 Transmission Acknowledgement	3 - 11
3.4.3.3 Misdirection of Messages	3 - 11
3.4.3.4 Disclosure	3 - 11
3.4.3.5 Unsolicited Messages	3 - 11
3.4.3.6 Retention of Documents	3 - 12
3.5 Electronic Mail	3 - 12
3.5.1 Authorised Users	3 - 12
3.5.2 Physical Protection	3 - 12
3.5.3 Logical Protection	3 - 12
3.5.4 Integrity of Content	3 - 13
3.5.5 Disclosure	3 - 13
3.5.6 Message Retention	3 - 13
3.5.7 Message Reception	3 - 13
3.5.8 Protection against Malicious Code	3 - 14
3.5.9 Security Labelling	3 - 14

	Page	
3.6	Mass Storage Media	3 - 14
3.6.1	Protection of Information in Storage Media	3 - 14
3.6.2	Environmental Considerations	3 - 14
3.6.3	Disposal of Storage Media	3 - 15
3.6.4	Non-Current Storage Media	3 - 15
3.6.5	Intellectual Property Rights	3 - 15
3.6.6	Vendors, Contractors, External Service Providers, Third Party Access	3 - 15
3.7	Business Resumption	3 - 16
3.7.1	Risk Analysis	3 - 16
3.7.2	Disaster Recovery/Contingency Plan	3 - 16
3.8	Public Sector ICT Security Incident Handling	3 - 18
3.8.1	Causes of Security Incidents	3 - 19
3.8.2	Handling Security Incidents	3 - 19
3.8.3	Developing Security Incidents Handling Capability	3 - 19
3.8.4	Issues to Consider When Setting an Incident Handling Capability	3 - 21
3.9	Public Sector ICT Security Awareness, Training, Acculturation And Education	3 - 21
3.9.1	Benefits of Public Sector ICT Security Awareness, Training, Acculturation and Education	3 - 22
3.9.2	Public Sector ICT Security Awareness	3 - 23
3.9.2.1	Techniques	3 - 24
3.9.3	Public Sector ICT Security Training & Acculturation	3 - 25
3.9.3.1	General Users	3 - 25
3.9.3.2	Specialised or Advanced Skills Users	3 - 26
3.9.4	Public Sector ICT Security education	3 - 26
3.9.5	Implementation	3 - 26
3.9.5.1	Understand the Core Business of the Organisation	3 - 26
3.9.5.2	Identify Gaps in Public Sector ICT Security Knowledge	3 - 27
3.9.5.3	Align Skill Gaps to Support the Organisation's Core Business	3 - 27
3.9.5.4	Identify Suitable Staffs	3 - 27
3.9.5.5	Allocate Financial Resources and Identify Training Location	3 - 27
3.9.5.6	Execute, Maintain and Evaluate Programme Effectiveness	3 - 28

	Page
3.10 Physical and Environmental ICT Security	3 - 29
3.10.1 Physical Security Perimeter	3 - 29
3.10.2 Physical Entry Controls	3 - 29
3.10.3 Secure Area	3 - 30
3.10.4 Working in a Secure Area	3 - 30
3.10.5 Site Protection for Data Centre and Computer Room	3 - 31
3.10.6 Equipment Protection	3 - 31
3.10.6.1 Hardware Protection	3 - 31
3.10.6.2 Storage Media Protection	3 - 31
3.10.6.3 Documentation Protection	3 - 32
3.10.6.4 Cabling Protection	3 - 32
3.10.7 Environmental Security	3 - 32
3.10.7.1 Environmental Control	3 - 32
3.10.7.2 Power Supply	3 - 33
3.10.7.3 Emergency Procedures	3 - 33
3.11 Cryptography	3 - 33
3.11.1 Symmetric (or Secret) Key Systems	3 - 34
3.11.2 Asymmetric (or Public) Key Systems	3 - 34
3.11.3 Key Management Issues	3 - 35
3.11.4 Disaster Cryptography and Cryptographic Disasters	3 - 35
3.11.4.1 Disaster Cryptography	3 - 35
3.11.4.2 Cryptographic Disasters	3 - 36
3.11.4.3 What to do in the event of a Cryptographic Disaster	3 - 36
3.12 Public Key Infrastructure (PKI)	3 - 37
3.13 Trusted Third Parties (TTP)	3 - 38
3.13.1 Assurance	3 - 38
3.13.2 Services of a TTP	3 - 39
3.13.3 Legal Issues	3 - 39
Chapter 4 TECHNICAL OPERATIONS	4 - 1
4.1 Computer Systems	4 - 1
4.1.1 Change Control	4 - 1
4.1.2 Equipment Maintenance	4 - 2
4.1.3 Disposal of Equipment	4 - 2

	Page
4.2 Operating Systems	4 - 2
4.2.1 Proprietary Issues	4 - 3
4.2.2 Shareware and Freeware Operating System Issues	4 - 3
4.2.3 Logical Access Control	4 - 3
4.2.3.1 Identification of Users	4 - 3
4.2.3.2 Authentication of Users	4 - 4
4.2.3.3 Limiting log-on Attempts	4 - 5
4.2.3.4 Unattended Terminals	4 - 6
4.2.3.5 Warning Messages	4 - 6
4.2.4 Audit Trails	4 - 6
4.2.5 Back-up	4 - 7
4.2.6 Maintenance	4 - 7
4.2.6.1 Patches and Vulnerabilities	4 - 7
4.2.6.2 Upgrades	4 - 7
4.3 Application System	4 - 8
4.3.1 Application Software	4 - 8
4.3.2 Databases	4 - 8
4.3.3 Systems which Employ Artificial Intelligence	4 - 9
4.3.4 Application Testing	4 - 9
4.3.5 Defective and Malicious Software	4 - 9
4.3.6 Change of Versions	4 - 10
4.3.7 Availability of Source Code	4 - 10
4.3.8 Unlicensed Software	4 - 10
4.3.9 Intellectual Property Rights	4 - 11
4.3.10 Malicious Code	4 - 11
4.3.11 Unauthorised Memory Resident Programs	4 - 11
4.3.12 Software Provided to External Parties	4 - 12
4.3.13 Software from External Sources	4 - 12
4.4 Network System	4 - 13
4.4.1 Securing a Network	4 - 13
4.4.1.1 Design of a Secure Network	4 - 13
4.4.1.2 Network Security Controls	4 - 14
4.4.2 Security of Network Equipment	4 - 15
4.4.2.1 Installation Security	4 - 15
4.4.2.2 Physical Security	4 - 15
4.4.2.3 Physical Access	4 - 16

	Page
4.4.2.4 Logical Access	4 - 16
4.4.2.5 Unauthorised Use of Equipment	4 - 17
4.4.2.6 Equipment Configuration	4 - 17
4.4.2.7 Equipment Maintenance	4 - 17
4.4.2.8 Disposal of Equipment	4 - 18
4.4.3 Securing Different Modes of Communications	4 - 18
4.4.3.1 Wired Network	4 - 18
4.4.3.2 Wireless Communication	4 - 19
4.4.3.3 Microwave Communication	4 - 20
4.4.3.4 Satellite	4 - 20
4.4.4 User Accessibility	4 - 20
4.4.4.1 Local Area Network	4 - 21
4.4.4.2 Remote Access	4 - 21
4.4.4.3 Dial-up Access	4 - 22
4.4.4.4 Virtual Private Networks	4 - 23
4.4.5 Connection with other Networks	4 - 24
4.4.5.1 Integrity of Connections	4 - 24
4.4.5.2 Firewalls	4 - 24
4.4.5.3 Public Users	4 - 27
4.4.5.4 Distributed Network Access	4 - 27
4.4.6 Protection during Transmission	4 - 28
4.4.6.1 Uploading & Downloading within Intranet	4 - 28
4.4.6.2 Uploading & Downloading to/from the Internet	4 - 28
4.4.7 Network Monitoring	4 - 29
4.4.7.1 Problems to be Monitored	4 - 29
4.4.7.2 How to Overcome Insider Attacks and Hackers	4 - 32
4.4.7.3 Monitoring Tools	4 - 33
4.5 Security Posture Assessment of ICT	4 - 34
Chapter 5 LEGAL MATTERS	5 - 1
5.1 Cyber Laws and Legal Implications	5 - 2
5.1.1 Digital Signature Act 1997	5 - 2
5.1.2 Computer Crime Act 1997	5 - 2
5.1.3 Telemedicine Act 1997	5 - 4
5.1.4 Copyright (Amendment) Act 1997	5 - 4
5.1.5 Communications and Multimedia Act 1998	5 - 5
5.1.6 Malaysian Communications & Multimedia Commission Act 1998	5 - 6

	Page
5.2 Crime Investigation	5 - 6
5.2.1 Definition of Computer Crime	5 - 6
5.2.1.1 Examples of Computer Essentials	5 - 6
5.2.1.2 Examples of Computer Non-Essentials	5 - 7
5.2.2 Evidence	5 - 7
5.2.2.1 Types of Evidence	5 - 7
5.2.3 Conducting Computer Crime Investigation	5 - 7
5.2.3.1 Detection and Containment	5 - 8
5.2.3.2 Report to Management	5 - 8
5.2.3.3 The Preliminary Investigation	5 - 8
5.2.3.4 Determine if Disclosure is Required	5 - 9
5.2.3.5 Investigation Considerations	5 - 9
5.2.3.6 Who should Conduct the Investigation	5 - 9

List of Tables

	Page
1. <i>Table 3.1:</i> Conventional vs. Digital Information Handling	3 - 1
2. <i>Table 3.2:</i> Public Sector ICT Security Awareness, Training and Education Programme	3 - 23
3. <i>Table 5.1:</i> Malaysian Cyber Laws	5 - 1
4. <i>Table 5.2:</i> List of Offences, Punishment and Enforcement	5 - 3
5. <i>Table 5.3:</i> List of Offences, Punishment and Enforcement	5 - 5

List of Figures

	Page
1. <i>Figure 1.1:</i> Various Levels of Details of Standards and Documents	1 - 3
2. <i>Figure 1.2:</i> Malaysian Public Sector Management of ICT Security Handbook (MyMIS) Roadmap	1 - 5
3. <i>Figure 2.1:</i> ICT Security in the System Life Cycle Phases	2 - 10
4. <i>Figure 3.1:</i> Handling Protection	3 - 1
5. <i>Figure 3.2:</i> Risk Analysis Model	3 - 17
6. <i>Figure 4.1:</i> Generic Network Security Architecture	4 - 14

List of Appendices

	Page
1. <i>Appendix A</i> : Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan	Appendix A - 1
2. <i>Appendix B</i> : Examples of Common Threats	Appendix B - 1
3. <i>Appendix C</i> : Examples of Common Abuses, Methods and Detection	Appendix C - 1
4. <i>Appendix D</i> : Example of Contents List for an Agency/ Department ICT Security Policy	Appendix D - 1
5. <i>Appendix E</i> : A Sample ICT Security Risk Management Process	Appendix E - 1
6. <i>Appendix F</i> : A Sample ICT Security Adherence Compliance Plan	Appendix F - 1
7. <i>Appendix G</i> : A Sample ICT Strategic Plan	Appendix G - 1
8. <i>Appendix H</i> : Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)	Appendix H - 1
9. <i>Appendix I</i> : A Sample Help Desk Reporting Form	Appendix I - 1
10. <i>Appendix J</i> : A Sample Employee Awareness Form	Appendix J - 1
11. <i>Appendix K</i> : A Sample Employee Security Checklist	Appendix K - 1
12. <i>Appendix L</i> : Disaster Recovery and Contingency Planning Checklist for ICT Systems	Appendix L - 1

References

Glossary