TECHNICAL CODE

REQUIREMENTS
FOR
INFORMATION AND NETWORK SECURITY

Developed by

Registered by

Registered date:

5 October 2016

© Copyright 2016

DEVELOPMENT OF TECHNICAL CODES

The Communications and Multimedia Act 1998 ('the Act') provides for Technical Standards Forum designated under section 184 of the Act or the Malaysian Communications and Multimedia Commission ('the Commission') to prepare a technical code. The technical code prepared pursuant to section 185 of the Act shall consist of, at least, the requirement for network interoperability and the promotion of safety of network facilities.

Section 96 of the Act also provides for the Commission to determine a technical code in accordance with section 55 of the Act if the technical code is not developed under an applicable provision of the Act and it is unlikely to be developed by the Technical Standards Forum within a reasonable time.

In exercise of the power conferred by section 184 of the Act, the Commission has designated the Malaysian Technical Standards Forum Bhd ('MTSFB') as a Technical Standards Forum which is obligated, among others, to prepare the technical code under section 185 of the Act.

A technical code prepared in accordance with section 185 shall not be effective until it is registered by the Commission pursuant to section 95 of the Act.

For further information on the technical code, please contact:

Malaysian Communications and Multimedia Commission (MCMC)
MCMC Tower 1
Jalan Impact, Cyber 6,
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel: +60 3 8688 8000
Fax: +60 3 8688 1000
http://www.mcmc.gov.my

OR

Malaysian Technical Standards Forum Bhd (MTSFB)
Malaysian Communications & Multimedia Commission (MCMC)
Off Persiaran Multimedia,
Jalan Impact
Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel: +60 3 8320 0300
Fax: +60 3 8322 0115
http://www.mtsfb.org.my

CONTENTS

Page

Committee Representation iii
FOREWORD iv
1. Scope 1
2. Normative References 1
3. Abbreviations and Definitions 1
3.1 Abbreviations 1
3.2 Definitions 1
4. Methodology 2
4.1 Organization Context 2
4.1.1 Understanding context of organization 2
4.1.2 Understanding the expectation of interested parties 2
4.1.3 Determining the scope of information and Network security management system 2
4.1.4 Information and Network Security Management System 2
4.2 Risk Management 2
4.2.1 General 2
4.2.2 Communication and consultation 3
4.2.3 Establish information security risk criteria 3
4.2.4 Information security risk assessment 3
4.2.5 Information and Network security risk treatment 4
4.3 Information and Network Security Objectives and planning to achieve them 4
5. Roles & Responsibilities 5
5.1 Leadership & Commitment 5
5.2 Policy 5
5.2.1 Roles, responsibilities within the organization and authorities 6
6. Support 6
6.1 Resources 6
6.2 Competence 6
6.3 Awareness 7
6.4 Communication 7
6.5 Documented information 7
6.5.1 General 7
6.5.2 Creating and Updating 7
6.5.3 Control of documented information 7
7. Operation 8
7.1 Operational planning and control 8
8 Performance Evaluation 8
8.1 Monitoring, measurement, analysis and evaluation 8
8.2 Internal Audit 9
8.3 Management review 9
9. Improvement 9
9.1 Nonconformity and corrective action 10
9.2 Continual improvement 10
Acknowledgements

Figure 1. Families of Control 11

Annexes

A Controls (reference to applicable controls and how these controls can be applied) 11
B (Informative Reference) 18

Committee Representation

Information Network and Security Working Group under the Malaysian Technical Standards Forum Bhd (MTSFB) which developed this Technical Code consists of representatives from the following organisations:

Altel Communications Sdn Bhd

Celcom Axiata Berhad

DiGi Telecommunications Sdn Bhd

Intel Corporation

Maxis Communications Berhad

Measat Broadcast Network Systems Sdn Bhd

Telekom Malaysia Berhad

TIME dotCom Berhad

TM Applied Business Sdn Bhd

Universiti Kuala Lumpur

Universiti Sains Malaysia

YTL Communications

FOREWORD

This technical code for Requirements of Information and Network Security ('this Technical Code') was developed pursuant to section 185 of the Act 588 by the Malaysian Technical Standards Forum Bhd ('MTSFB') via its Information Network and Security Working Group.

This Technical Code shall continue to be valid and effective until reviewed or cancelled.

MCMC MTSFB TC G009:2016

REQUIREMENTS FOR INFORMATION AND NETWORK SECURITY

1. Scope

This Technical Code has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an information and network security management system within the context of an organization. This Technical Code also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirement set out in this Technical Code are generic and intended to be applicable to all organizations, regardless of size, type or nature. Excluding any of the requirements specified in Sections 4 to 9 is not acceptable when an organization claims conformity to this Technical Code.

2. Normative References

The following normative references are indispensable for the application of this Technical Code. For dated references, only the edition cited applies. For undated references, the latest edition of the normative references (including any amendments) applies.

ISO/IEC 27001:2013, *Information technology - Security techniques - Information security management systems - Requirements*

ISO/IEC 27002:2013, *Information technology - Security techniques - Code of practice for information security controls*

ISO/IEC 27005:2011, *Information technology - Security technique - Information security risk management.*

NIST SP 800-100, *Information Security Handbook: A Guide for Manager, Oct 2006*

NIST SP-800-39, *Managing Information Security Risk*, March 2011

NIST SP-800-53, *Security and Privacy Controls for Federal Information Systems and Organization, Revision 4.*

Act 709 - *Personal Data Protection Act, Malaysia*, 2010

3. Abbreviations and Definitions

3.1 Abbreviations

For the purposes of this Technical Code, the following abbreviation applies.

CISO	Chief Information Security Officer
CSIRT	Computer Security Incident Response Team
INS	Information and Network Security

3.2 Definitions

For the purposes of this Technical Code, the following definition applies.

Teleworking	Working from remote location i.e. home

Mobile Devices	Devices that provides computing and mobility, such as mobile phones.

4. Methodology

Risk management comprises of the following activities:

4.1 Organization context

4.1.1 Understanding context of organization.

The organization shall determine internal and external issues that are relevant to its purpose and that affects its ability to achieve the intended outcome(s) of its information and network security management system.

4.1.2 Understanding the expectation of interested parties

The organization shall determine:

a) interested parties that are relevant to the information and network security management systems; and

b) the requirements of these interested parties relevant to the information and network security.

NOTE. The requirements of interested parties may include legal and regulatory requirements and contractual obligations.

4.1.3 Determining the scope of information and network security management system

The organization shall determine the boundaries and applicability of the information and network security management system to establish its scope. The determination of scope shall take the following into consideration.

a) The internal and external issues referred to, in Section 4.1;

b) The requirements referred to in Section 4.2; and

c) Interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.

The scope shall be available as documented information.

4.1.4 Information and Network security management system

The organization shall establish, implement, maintain and continually improve an information and Network security management system, in accordance with the requirements of this Technical Code.

4.2 Risk management

4.2.1 General

When planning for the information and Network security management system, the organization shall consider the issues referred to in Section 4.1 and determine the risks and opportunities that need to be addressed to:

a) ensure information and Network security management system can achieve its intended outcome(s);

b) prevent, or reduce undesired results to business and objectives of the program; and

c) achieve continual improvement.

The organization shall plan:

a) actions to address these risks and opportunities; and

b) how to

   i. integrate and implement the actions into its information and Network security management system processes; and

   ii. evaluate the effectiveness of these actions.

4.2.2 Communication and consultation

Engagement sessions with both internal and external stakeholders shall occur throughout the information security risk management process. Communication and consultation with stakeholders is important as stakeholders make judgements based on their perceptions of risk which can vary in values, needs, assumptions, concepts and concerns.

4.2.3 Establish information security risk criteria

The organization shall establish the external and internal context of its information security risk management process. This includes the establishment of the information security risk acceptance criteria and the criteria for performing information security risk assessment.

4.2.4 Information security risk assessment

Risk assessment is an integral part of information security risk management. It comprises of risk identification, risk analysis and risk evaluation.

a) Risk assessment shall establish and maintain information and Network security risk criteria that includes:

   i. the risk acceptance criteria; and

   ii. criteria for performing information and Network security risk assessment.

b) Ensures that repeated information security risk assessments produce consistent, valid and comparable result

c) Identifies the information and Network security risks.

   i. apply the information and Network security risk assessment process to identify risks associated with the confidentiality, integrity and availability for information within the scope of the information and Network security management system; and

   ii. identify risk owners.

d) analyze the information and Network security risks

   i. assess the potential consequences that would result if the risks identified materialize;

   ii. assess the realistic likelihood of the occurrence of the risks identified; and

   iii. determine the level of risks.

e) Evaluate the information and Network security risks:

   i. Compare the result of risk analysis with the risk criteria established in 4.2.3; and

ii. Prioritize analyzed risk for risk treatment.

4.2.5 Information and Network security risk treatment

The organization shall define and apply an information and Network security risk treatment process to:

a) Select appropriate information and Network security risk treatment options, taking account of the assessment result;

b) Determine all controls that are necessary to implement the information and Network security risk treatment option(s) chosen

NOTE. Organizations can design controls as required, or identify them from any source.

c) Compare the controls determined in 4.2.5 b) above with those in Annex A and verify that no necessary controls have been omitted;

NOTES:

1 Annex A contains a comprehensive list of control objectives and controls. Users of this Technical Standards are directed to Annex A to ensure that no necessary controls are overlooked.

2 Control objectives are implicitly included in the controls chosen. The control objectives and controls listed in Annex A are not exhaustive and additional control objectives and controls may be needed.

d) Produce a statement of Applicability that contains the necessary controls and justifications for inclusions, whether they are implemented or not, and the justification for exclusion of controls from Annex A;

e) Formulate an information and Network security risk treatment plan; and

f) Obtain risk owner's approval of the information and Network security risk treatment plan and acceptance of the residual information and Network security risk.

The organization shall retain documented information about the information and Network security risk assessment process.

4.3 Information and Network security objectives and planning to achieve them

The organization shall establish information and Network security objectives at relevant functions and levels.

The information and Network security objectives shall:

a) be consistent with the information and Network security policy;

b) be measurable (if applicable);

c) take into account applicable information and Network security requirements, and results from risk assessment and risk treatment;

d) be communicated; and

e) be updated as appropriate.

The organization shall retain documented information on the information and Network security objectives.

When planning how to achieve its information and Network security objectives, the organization shall determine:

a) What will be done;

b) What resources will be required;

c) Who will be responsible;

d) When it will be completed; and

e) How the results will be evaluated.

5. Roles and responsibilities

5.1 Leadership and commitment

Top management shall demonstrate leadership and commitment with respect to the information and Network security management system by:

a) ensuring the information and Network security policy and the objectives are established and are compatible with the strategic direction of the organization;

b) ensuring the integration of the information and Network security requirements into the organization's process;

c) ensuring that the resources needed for the information and Network security management system are available;

d) communicating the importance of effective information and Network security management and of confirming to the information and Network security management requirements;

e) ensuring that the information and Network security management system achieves the intended outcome(s);

f) directing and supporting persons to contribute the effectiveness of the information and Network security management system;

g) promoting continual improvement; and

h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibilities.

5.2 Policy

Organization leadership shall establish a management framework to initiate and control the implementation of information and Network security. Management shall approve the information and Network security policy, assignment of security roles, coordinate and review of the implementation of security across the organization.

Each policy shall have an owner who has approved management responsibility for the development, review and evaluation of the policies. Reviews include assessing opportunities for improvement of the organization's policies and approach to managing information security in response to changes to the organizational environment, business circumstances, legal conditions or technical environment.

Top management shall establish an information and Network security policy that:

a) is appropriate to the purpose of the organization;

b) includes information and Network security objectives or provide the framework for setting the information and Network security objectives;

c) includes a commitment to satisfy applicable requirements related to information and Network security; and

d) include a commitment to continual improvement of the information and Network security management system.

The information and Network security policy shall:

a) be available as documented information;

b) be communicated within the organization; and

c) be available to interested parties, as appropriate.

5.2.1 Roles, responsibilities within the organization and authorities

Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated.

Top management shall assign the responsibilities and authority for:

a) ensuring that the information and Network security management system conforms to the requirements of this Technical Standard; and

b) reporting on the performance of the information and Network security management system to top management.

NOTE. Top management may also assign responsibilities and authorities for reporting performance of the information and Network security management system within the organization.

These are the functions shall be assigned in the applicable organization:

a) Regulatory/Authority Contact;

b) Information and Network Security responsibility; and

c) Risk Management.

6. Support

6.1 Resources

The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information and Network security management system.

6.2 Competence

The organization shall:

a) Determine the necessary competence of person(s) doing work under its control that affects the performance of information and Network security;

b) ensure that these persons are competent on the basis of appropriate education, training or experience;

c) where applicable, take action to acquire the necessary competence, and evaluate effectiveness of the action taken; and

d) retain appropriate documented information as evidence of competence.

NOTE. Applicable action may include, for example: the provision of training to, the mentoring of, or the re-assignment of current employees; or the hiring or contracting of competent persons.

6.3 Awareness

Persons doing work under the organization's control shall be aware of:

a) Information and Network security policy;

b) their contribution to the effectiveness of the information and Network security management system, including the benefits of improved information and Network security performance; and

c) the implications of not conforming to the information and Network security management system.

6.4 Communication

The organization shall determine the need for internal and external communications relevant to information and Network security management system including:

a) on what to communicate;

b) when to communicate;

c) with whom to communicate;

d) who shall communicate; and

e) the process by which communication shall be effected.

6.5 Documented information

6.5.1 General

The organization's information and Network security management shall include:

a) Documented information required by this Technical Standard; and

b) Documented information determined by the organization as being necessary for the effectiveness of the information and Network security management system

The extent of documented information for an information and Network security management system can differ from one organization to another due to:

a) size and type of activities, process, products and services of an organization;

b) the complexity of processes and their interactions; and

c) the competence of the persons.

6.5.2 Creating and Updating

When creating and updating documented information the organization shall ensure appropriate:

a) identification and description (e.g. title, date, author or reference number);

b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and

c) review and approval for suitability and adequacy.

6.5.3 Control of documented information

Documented information required by the information and Network security management system and by this Technical Code shall be controlled to ensure:

a) it is available and suitable for use, where and when it is needed; and

b) it is adequately protected (e.g. from loss of confidentiality, improper use or loss of integrity).

For the control of documented information, the organization shall address the following activities as applicable:

a) distribution, access, retrieval and use;

b) storage and preservation, including the preservation of legibility;

c) control of changes (e.g. version control); and

d) retention and disposition.

Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information and Network security management system, shall be identified as appropriate, and controlled.

NOTE. Access implies a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information, etc.

7. Operation

7.1 Operational planning and control

The organization shall plan, implement and control the processes needed to meet information and Network security requirements, and to implement the actions determined in section 4.1. The organization shall also implement plans to achieve information and Network security objectives determined in section 5.2.

The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned.

The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization shall ensure that outsourced processes are determined and controlled.

8 Performance Evaluation

8.1 Monitoring, measurement, analysis and evaluation

The organization shall evaluate the information security performance and the effectiveness of the information and Network security management system.

The organization shall determine:

a) what needs to be monitored and measured, including information and Network security processes and controls; and

b) the methods for monitoring, measurement, analysis and evaluation, as applicable to ensure valid results.

NOTE. The methods selected should produce comparable and reproducible results to be considered valid.

The organization shall retain appropriate documented information as evidence of the monitoring and measurement results.

8.2 Internal audit

The organization shall conduct internal audits at planned intervals to provide information on whether the information and Network security management system:

a) conforms to

   i. the organization's own requirements for its information and Network security management system; and;

   ii. the requirements of this Technical Code.

b) is effectively implemented and maintained.

The organization shall:

a) plan, establish, implement and maintain an audit program(s), including the frequency, method, responsibilities, planning requirements and reporting. The audit program(s) shall take into consideration the importance of the processes concerned and the result of the previous audit;

b) define the audit criteria and scope of each audit;

c) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process

d) ensure that the results of the audits are reported to the relevant management; and

e) retain documented review information as evidence of the audit program(s) and the audit results

8.3 Management review

Top management shall review the organization's information and Network security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

The management review shall include considerations of:

a) the status of actions from previous management reviews;

b) changes in external and internal issues that are relevant to the information and Network security management system;

c) feedback on the information and Network security performance, including trends in:

   i. nonconformities and corrective actions;

   ii. monitoring and measurement results;

   iii. audit results; and

   iv. fulfillment of information and Network security objectives

d) feedback from interested parties;

e) results of risk assessment and status of risk treatment plan; and

f) opportunities for continual improvement

The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information and Network security management system.

The organization shall retain documented information evidence of the results of management reviews.

9. Improvement

9.1 Nonconformity and corrective action

When nonconformity happens, the organization shall:

a) react to the nonconformity, and as applicable
   i. take action to control and correct it; and
   ii. deal with the consequences

b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere by:
   i. review the nonconformity;
   ii. determining the causes of the nonconformity; and
   iii. determining if similar nonconformities exist, or could potentially occur.

c) implement any action needed;

d) review the effectiveness of any corrective action taken; and

e) make changes to the information and Network security management system, if necessary.

Corrective actions shall be appropriate to the effects of the nonconformities encountered. The organization shall retain documented information as evidence of:

a) the nature of the nonconformities and any subsequent actions take, and

b) the results of any corrective action.

9.2 Continual improvement

The organization shall continually improve the suitability, adequacy and effectiveness of the information and Network security management system.

Annex A
(normative)

Controls
(reference to applicable controls and how these controls can be applied)

The following controls apply based on identified risks in line with Section 4.3. The controls are divided into 4 families of controls.

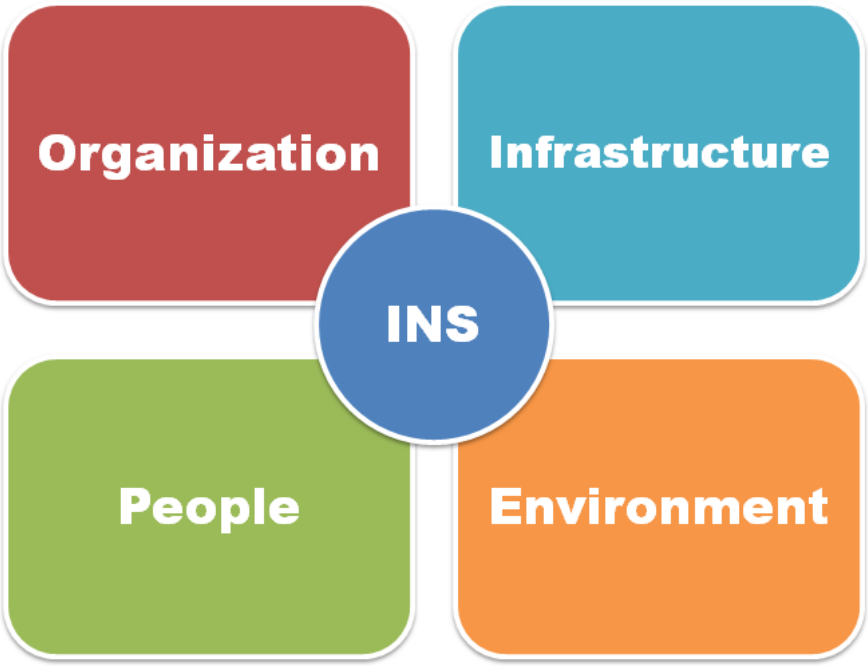

Figure 1. Families of Control

A.1 Organization

This family of control focuses on organizational readiness for Information and Network Security. A business shall have a formal and systematic approach to implementing and maintaining an effective Information and Network Security Program.

A.1.1 Information and Network security policy

A policy that encompasses information security requirements that provides the management direction and intent based on business requirements that are:

a) Guided by relevant laws and regulatory requirements; and

b) Reviewed at planned intervals to ensure congruence towards the dynamic landscape of business, appropriateness based on current technologies and effectiveness of controls and requirements.

A.1.2 Business Continuity Management

Organization survival depends on having a solid business continuity plan. This plan needs to incorporate the information and Network security elements to ensure completeness and comprehensiveness of the plan, in line with the organization's Information and Network Security Program.

a) Establish, maintain and implement effective plans for emergency response and post disaster recovery to ensure availability and continuity of operations in emergency situations; and

b) To review, verify and evaluate the plans at regular intervals to ensure effectiveness and validity.

c) Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.

A.1.3 Information and Network security compliance

Organizations are bound by the laws of the land, which requires compliance by identifying and understanding the legal, statutory and contractual obligations pertaining to information and Network security.

a) Identify, document and keep up to date applicable legal, statutory and contractual obligations.

b) Protect records/information, personal and sensitive data in accordance with legal, regulatory, contractual and business requirements.

c) Procedures shall be established in relation to management of intellectual property rights and use of proprietary software products.

d) Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.

e) Privacy and personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.

f) The organization's approach to managing information and Network security and its implementation shall be reviewed independently at planned internals or when significant changes occur.

g) Managers of the organization shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.

h) Information systems shall be regularly reviewed for compliance with the organization's information and Network security policies and standards.

A.1.4 Organization of information security

a) Establishing a management framework to initiate and control the implementation and operation of information security within the organization.

   i. Information security roles and responsibilities;

   ii. Segregation of duties;

   iii. Contact with authorities;

   iv. Contact with special interest groups; and

   v. Information security in project management.

b) Ensure the security of teleworking and use of mobile devices.

   i. Mobile device policy; and

   ii. Teleworking.

A.1.5 Information security incident management

a) Security incident management will assist in responding appropriately to security incidents, including applying appropriate remedies and future prevention measures;

b) Security events and weaknesses are communicated in a manner allowing timely corrective action to be taken;

c) Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to security incidents;

d) Incidents related to information and Network security shall be reported through appropriate management channels as quickly as possible.

e) Evidence relating to a security violation must be properly collected, documented and preserved; and

f) All incidents must be properly investigated and analyzed. Corrective action must be taken to recover from security violations. Subsequently, preventative measures must be taken to avoid the reoccurrence of the incident. Reviews must be done on a periodic basis (as part of operational procedural review) to evaluate the effectiveness of the controls, lesson learned and disciplinary action taken.

g) Knowledge gained from incidents shall be used to reduce the likelihood or impact of future incidents.

A.2 Infrastructure

A.2.1 Asset management

Business performance relies on its assets. Business assets may comprise of physical or virtual elements, network equipment, server hardware and human capital.

a) Assets pertaining to information and processing shall be identified;

b) Assets shall be drawn and maintained in an inventory with the owners identified, returned upon termination of employment, contract or agreement; and

c) Acceptable use of asset rules shall be identified, documented and implemented.

A.2.2 Information management

a) Information shall be classified, labelled and handled in accordance to value, sensitivity, criticality and legality;

b) Procedures shall be implemented for the management of information lifecycle including asset handling;

c) Test data shall be carefully selected, protected and controlled; and

d) Test data derived from production data shall be protected equivalent to production data.

A.2.3 Media management

a) Procedures shall be implemented for the management and disposal of storage media based on the classification scheme; and

b) Media containing information shall be protected against unauthorized access, misuse or corruption.

A.2.4 Access control

a) An access control policy shall be drawn up, documented and reviewed based on business and information and Network security requirements; and

b) Access to network and services shall only be provided for those who have been specifically authorized to do so.

A.2.5 User access management

a) A formal process for user registration and de-registration shall be implemented to enable assignment of account and access rights;

b) A formal process for user access provisioning shall be implemented to assign or revoke access rights for all types of users, systems and services;

c) The allocation and use of privileged access rights shall be restricted and controlled;

d) The allocation of secret authentication information shall be controlled through a formal management process;

e) Users shall be required to adhere to organization's practices in the use and management of secret authentication information;

f) The allocation and use of privileged access rights shall be restricted and controlled;

g) Asset owners shall formally review user's access rights at regular intervals; and

h) A formal process to remove access rights of all employees and external party users to information, systems, infrastructure and services upon termination of their employment, contract or agreement, or adjust upon change is implemented and managed.

A.2.6 Systems, services and application access control

a) Access to systems, services and application shall be restricted in accordance with the access control policy of the organization;

b) Access to systems, services and applications shall be controlled by a secure log-on procedure where required by the access control policy;

c) When passwords are used, a password management system shall be interactive and shall ensure quality/strong passwords; and

d) Use of privileged systems which provide capabilities to override system and application controls shall be restricted and tightly controlled.

e) Program source code access shall be restricted

A.2.7 Cryptography

a) A policy on the use of cryptographic controls for protection of information shall be developed and maintained, based on legal/regulatory obligations and other industry requirements;

b) Cryptographic key management policy on the use, protection and lifetime shall be developed and implemented to manage its lifecycle; and

c) Cryptographic controls shall be used in compliance to all relevant legislations, regulations and contracts/agreements and shall be in accordance with industry best practices.

A.2.8 Information and Network security in operations

a) Operating Procedures shall be documented and made available;

b) Changes made in the Operations environment shall be controlled, managed and documented;

c) Resources used in Operations shall be monitored, tuned and protections made of future capacity requirements to ensure meeting the required system performance; and

d) Environments of development, testing and operations shall be kept separate to reduce risks of unauthorized access or changes.

A.2.9 Malicious software protection

a) Sufficient detection, prevention and recovery controls to protect against malware shall be implemented; and

b) Awareness on malware shall be made to all organization users.

A.2.10 Logging and monitoring

a) Event logs shall be enabled to record system activities, exceptions, faults and security events;

b) Event logs shall be kept and regularly reviewed;

c) Logs and logging facilities shall be protected against unauthorized access and tampering;

d) Clocks of all relevant systems/ information andinfrastructure shall be synchronized to an organization authorized reference time source; and

e) Administrative and Operator access shall be logged and the logs regularly reviewed and sufficiently protected.

A.2.11 Control of operational software

Installation of software on operational system shall be controlled based on installation and implementation procedures.

A.2.12 Technical vulnerability management

a) Information about technical vulnerabilities of systems/network/infrastructure shall be obtained in timely manner, to ensure that exposure to such vulnerabilities are evaluated and necessary measures taken to address the risk; and

b) Procedures governing installation of software by users shall be established and implemented.

A.2.13 Information and Network audit

Activities involving verification of operational systems and audit requirements shall be planned and agreed to minimize disruption to business processes.

A.2.14 Backup

Backup copies of information and required software shall be taken and tested regularly according to an agreed backup policy.

A.2.15 Network communications security management

a) Networks shall be managed and controlled to protect information in systems, application and services;

b) Network service agreements for both in-source and outsourced environment shall contain requirements of security mechanisms, service levels and management of all network services; and

c) Networks shall be segregated based on groups of information services, users and systems.

A.2.16 Information transfer

a) Formal policies, procedures and controls shall be in place to protect information transfer through the use of all types of communication facilities;

b) Formal agreements shall address the secure transfer of information between organization and external parties;

c) Electronic messaging that contains information for the organization shall be protected; and

d) Non-disclosure or confidentiality agreements reflecting the need of the organization to protect information shall be identified, regularly reviewed and documented.

A.2.17 Security requirements of systems

a) Information and Network security related requirements shall be included in the requirements for new systems or existing system enhancements; and

b) Information pertaining to application service and service transactions shall be protected to maintain confidentiality, integrity and availability.

A.2.18 Security requirements for development and support processes

a) Procedure for development of systems, software and services shall be established and applied to developments within the organization;

b) Changes to systems, software and services within the development lifecycle shall be controlled through a formal change control procedure;

c) Business critical applications, software and services shall be reviewed and tested to ensure there are no adverse impact on operations or security when operating platforms are changed;

d) All changes to systems, software and services shall be strictly controlled; modifications to packages shall be discouraged, limited to necessary changes;

e) Secure systems engineering principles shall be established, documented, maintained and applied to any implementation efforts;

f) Procedure for establishing and protecting secure development environment for development and integration efforts that cover the entire system development lifecycle shall be drawn up;

g) Security functionality testing shall be carried out during development;

h) Organization shall supervise and monitor activities of outsourced system development; and

j) Acceptance testing criteria and programs shall be established for new systems, upgrades and new versions.

A.2.19 System acquisition, development and maintenance

a) All security requirements should be identified and analyzed at the requirements phases of a project and justified, agreed, documented, tested and delivered as part of the overall business case for an information system; and

b) Project and support environments should be strictly controlled. Designated Owner shall be responsible for the security elements of the project or support processes.

A.3 People

A.3.1 Human resource security

a) The organization shall ensure employees and contractors understand and comply with their responsibilities and are suitable for the roles for which they are assigned; and

b) The organization shall adhere to its security-related responsibilities in personnel-related processes, inclusive of:

   i. Screening;

   ii. Terms and conditions of employment;

   iii. Management responsibilities;

   iv. Information security awareness, education and training;

   v. Disciplinary process; and

   vi. Termination or change of employment responsibilities.

A.3.2 Supplier relationships

a. The organization shall ensure that its suppliers and partners are aware of their security obligations, and that these suppliers and partners maintain a security standard that is suitable to prevent breaches in security.

b. The supplier agreements shall include requirements for information and Network security and address information and Network security risks associated with information technology services and product supply chain.

c. Organization shall regularly monitor, review, audit supplier service delivery.

d. Changes to the provision of services by suppliers, including maintaining and improving existing information and Network security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.

A.4 Environment

A.4.1 Physical and environmental security

a) The organization shall ensure that physical and environmental security controls are identified, and these controls are implemented;

b) Physical and environmental security measures should prevent unauthorized physical access, damage and interference to the organization's premises and information; and

c) Security perimeters should be clearly defined, and the siting and strength of each of the perimeter shall depend on the security requirements of the assets within the perimeter and the results of a risk assessment.

d) Equipment, software or information shall not be taken off-site without prior authorization.

e) All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or security overwritten prior to disposal or re-use.

Annex B

(informative)

B.1 Organization shall also consider the establishment of organizational CSIRT and Security Operation Centre to continuously monitor and mitigate security risks, threats and vulnerabilities.

Acknowledgements

Members of the Information Network and Security Working Group

Dr. Suresh Ramasamy (Chairman)	DiGi Telecommunications Sdn Bhd
Mr. Steven Rosen (Vice Chairman)	YTL Communications
Ms. Azleyna Ariffin / (Secretary)	Independent Expert
Ms. Rafeah Omar	Telekom Malaysia Bhd
Mr. Rosli Sukri	Altel Communications Sdn Bhd
Ms. Hafiza /	Celcom Axiata Berhad
Mr. Jafri	
Mr. Alex Kuek Teck Seng /	DiGi Telecommunications Sdn Bhd
Mr. Ramany Kandasamy	
Ms. Noorul Halimin Mansur	Independent Expert
Dr. Tan Tat Kin	Intel Corporation
Mr. Rakuram Gandhi /	Maxis Communications Berhad
Mr. Sivananthan Nithiananthan	
Mr. Abd Razak Abd Hamid /	Measat Broadcast Network Systems Sdn Bhd
Mr. Mohamad Isa Mohd Razhali	
Mr. Senthilvasan Muthan	Measat Satellite Systems Sdn Bhd
Mr. Arief Khalid Supian /	Telekom Malaysia Berhad
Mr. Nuremi Abd Halim /	
Mr. Wan Rafizah B Mohamed Ariffin	
Mr. Md Ridhwan Bin A Razak/	TIME dotCom Berhad
Mr. Sri Kanth a/l Rajalingam	
Mr. Thaib Mustafa	TM Applied Business Sdn Bhd
Prof. Dr. Shahrulniza Musa	Universiti Kuala Lumpur
Assoc Prof. Dr. Aman Jantan	Universiti Sains Malaysia
Mr. Desmond Hong /	YTL Communications
Mr. Ionut Gioglovan /	
Mr. Mohd Hanafi B Mohd Nasir /	
Mr. Shrinivas Kulkarni	