# SECURITY GUIDELINES

## FOR INFORMATION AND NETWORK SECURITY MANAGEMENT

**Edition: April 2023**

**The 35th APT Standardization Program Forum (ASTAP-35)**
**17 – 20 April 2023**
**Bangkok, Thailand**

***(Source: ASTAP-35/OUT-11)***

**No. APT/ASTAP/REPT-53**

**Table of Contents**

# SECURITY GUIDELINES FOR INFORMATION AND NETWORK SECURITY MANAGEMENT

## 1. Scope

This document is to provide security guidelines for establishing, implementing, maintaining, and continually improving an information and network security management within the context of an organization. The guideline includes the assessment and treatment of information security risks tailored to the needs of the organization. The guideline set out in this document are generic and intended to be applicable to all organizations, regardless of size, type, or nature.

## 2. References

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

| | |
|---|---|
| ITU-T X.1051\| ISO/IEC 27011 | Information technology – Security techniques – Guideline for information security controls based on ISO/IEC 27002 for telecommunications organizations |

## 3. Abbreviations

| | |
|---|---|
| CISO | Chief Information Security Officer |
| CSIRT | Computer Security Incident Response Team |
| INS | Information and Network Security |
| IP | Internet Protocol |
| OWASP | Open Web Application Security Project |
| SOC | Security Operation Centre |
| TCP | Transmission Control Protocol |
| UDP | User Datagram Protocol |

## 4. Terms and Definitions

| | |
|---|---|
| Teleworking | Working from remote location i.e. home |
| Mobile Devices | Devices that provide computing and mobility such as mobile phones. |

Other terms and definition as stated in ISO/IEC 27011 is referred.

## 5. Requirements

### 5.1 Organisation context

#### 5.1.1 Understanding context of organization

The organisation should determine internal and external issues that are relevant to its purpose and that affects its ability to achieve the intended outcome(s) of its INS management system.

#### 5.1.2 Understanding the expectation of interested parties

The organisation should determine:

a) interested parties that are relevant to the INS management systems; and

b) the requirements of these interested parties relevant to the INS.

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

#### 5.1.3 Determining the scope of INS management system

The organisation should determine the boundaries and applicability of the INS management system to establish its scope. The determination of scope should take the following into consideration:

a) the internal and external issues referred in 5.1;

b) the requirements referred in 5.2; and

c) interfaces and dependencies between activities performed by the organisation, and those that are performed by other organisations.

The scope should be available as documented information.

#### 5.1.4 INS management system

The organisation should establish, implement, maintain and continually improve an INS management system, in accordance with the requirements of this guideline.

## 5.2 Risk management

### 5.2.1 General

When planning for the INS management system, the organisation should consider the issues referred in 5.1 and determine the following risks and opportunities that need to be addressed:

a) security management system can achieve its intended results(s);

b) enhance desirable effects;

c) prevent, or reduce undesired effects; and

d) achieve improvement.

The organisation should plan the actions to address these risks and opportunities and identify the following items:

a) integrate and implement the actions into its INS management system processes; and

b) evaluate the effectiveness of these actions.

### 5.2.2 Risk management process

The main purpose of the risk management process is to enable the organisation to assess the existing or potential risks that may be faced, evaluate the risks by comparing the risk analysis results with the established risk criteria, and treat such risks using the risk treatment options. The organisation should use such process when making decisions.

Figure 1 shows the steps for an effective implementation/integration of the risk management process are as follows:

a) communication and consultation;

b) scope, context and criteria;

c) risk assessment;

d) risk treatment;

e) monitoring and review; and

f) recording and reporting risk.

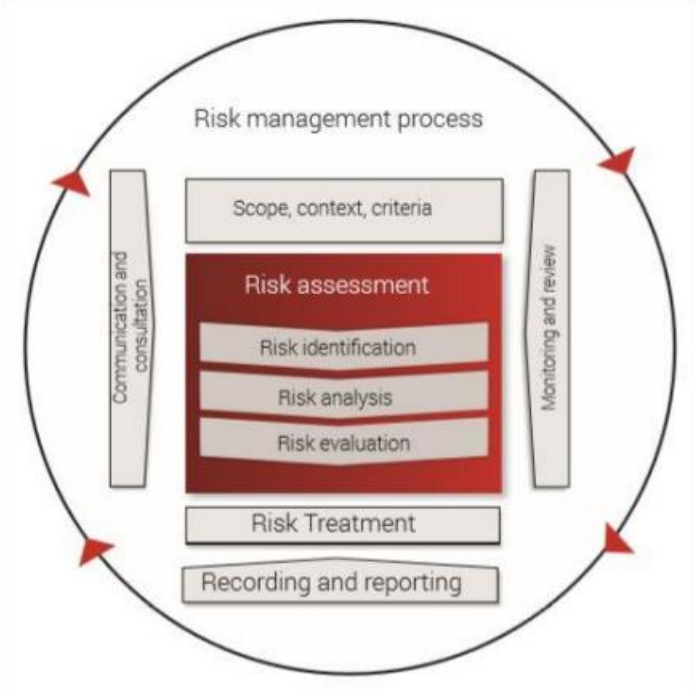


**Figure 1. Risk Management Process**

### 5.2.3 Communication and consultation

Proper risk management requires structured and on-going communication and consultation with those affected by the organisation's operations. The communication seeks to promote awareness and understanding of risk and the means to respond to it. Consultation involves obtaining feedback and information to support decision-making which the activities in this step are as follows:

a) bringing different areas of expertise together for each step of the risk management process;

b) ensuring different views are considered when defining risk criteria and evaluating risks;

c) providing sufficient information to facilitate risk oversight and decision-making; and

d) building a sense of inclusiveness and ownership among those affected by risk.

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

### 5.2.4 Scope, context and criteria

The organisation should define the purpose and scope of its risk management activities and determine the objectives of the risk management process and the specific objectives of risk assessment. When establishing the context, the organisation should take into account the organisation's external context (political, social, etc.) and internal context (objectives, strategies,

structures, ethics, discipline, etc.). The organisation's context must be understood before the full range of risks can be identified. This includes the establishment of the information security risk acceptance criteria and the criteria for performing INS risk assessment.

### 5.2.5 INS risk assessment

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

#### 5.2.5.1 Risk identification

Risk identification is about the creation of a comprehensive list of risks (both internal and external) that the organisation faces and can involve input from sources such as historical data, theoretical analysis, expert options, and stakeholder's needs. The identification of risks should be a formal, structured process that includes risk sources, events, their causes and their potential consequences.

The organisation should establish and maintain security risk criteria that includes:

a) the risk acceptance criteria; and

b) criteria for performing INS risk assessment.

The organisation should ensure that repeated information security risk assessments produce consistent, valid and comparable results. The organisation should identify INS risks by:

a) applying the INS risk assessment process to identify risks associated with the confidentiality, integrity and availability for information within the scope of the INS management system; and

b) identifying risk owners.

#### 5.2.5.2 Risk analysis

The organisation should analyse each risk that was identified in the 5.2.5.1. Based on the level of risk that is determined after the risk analysis, the organisation can define whether the risk is acceptable or not. As so, if the risk turns out to be unacceptable, the organisation can take actions to modify the risk to correspond to the acceptable level of risk.

The organisation should use a formal technique to consider the consequence and likelihood of each risk, and these techniques can be qualitative, semi-quantitative, quantitative, or a combination thereof, based on the circumstances and the intended use.

Analyse the INS risks includes:

a) assess the potential consequences (impact) that would result if the risks identified materialise;

b) assess the realistic likelihood of the occurrence of the risks identified; and

c) determine the level of risks.

#### 5.2.5.3 Risk evaluation

This step offers the organisation the opportunity to have a mechanism that helps them rank the relative importance of each risk, so that a treatment priority can be established.

Evaluate the INS risks:

a) compare the result of risk analysis with the risk criteria established in 5.2.4; and

b) prioritise analysed risk for risk treatment.

### 5.2.6 Risk treatment

The organisation should define and apply an INS risk treatment process to:

a) select appropriate INS risk treatment options, taking account of the assessment result;

   NOTE: There are 4 options available for risk treatment options: risk modification, risk retention, risk avoidance and risk sharing.

b) determine all controls that are necessary to implement the INS risk treatment option(s) chosen;

   NOTE: Organisations can design controls as required or identify them from Annex A or any source.

c) formulate an INS risk treatment plan; and

d) obtain risk owner's approval of the INS risk treatment plan and acceptance of the residual INS risk.

The organisation should retain documented information about the INS risk assessment process.

### 5.2.7 Monitoring and review

Organisation should monitor and review the risk treatment plan by:

a) examining the progress of treatment plans; and

b) monitoring the established controls and their effectiveness.

### 5.2.8 Recording and reporting

Organisation should record and report the risk management activities and outcomes pertaining to those activities throughout the organisation and providing the necessary basis and information for making informed decisions.

### 5.3 Objectives and planning

The organisation should establish INS objectives at relevant functions and levels. The INS objectives should consider the following items:

a) be consistent with the INS policy;

b) be measurable (if applicable);

c) take into account applicable INS requirements, and results from risk assessment and risk treatment;
d) be communicated; and

e) be updated as appropriate.

The organisation should retain documented information on the INS objectives.

When planning how to achieve its INS objectives, the organisation should determine the following questions:

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.

## 6. Roles and responsibilities

### 6.1 Leadership and commitment

Top management should demonstrate leadership and commitment with respect to the INS management system by:

a) appointing a Chief Information Security Officer (CISO) or equivalent who is an independent authority and reports to Board of Directors, that is responsible for the overall INS for the organisation;

b) ensuring the INS policy and the objectives are established and are compatible with the strategic direction of the organisation;

c) ensuring the integration of the INS requirements into the organisation's process;

d) ensuring that the resources needed for the INS management system are available;

e) communicating the importance of effective INS management and of confirming to the INS management requirements;

f) ensuring that the INS management system achieves the intended outcome(s);

g) directing and supporting persons to contribute the effectiveness of the INS management system;

h) promoting continual improvement; and

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

### 6.2 Policy

Organisation leadership should establish a management framework to initiate and control the implementation of INS. Management should approve the INS policy, assignment of security roles,
coordinate and review of the implementation of security across the organisation.

Each policy should 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 organisation's policies and approach to managing information security in response to changes to the organisational environment, business circumstances, legal conditions or technical environment.

Top management should establish an INS policy that:

a) is appropriate to the purpose of the organisation;

b) includes INS objectives or provide the framework for setting the INS objectives;

c) includes a commitment to satisfy applicable requirements related to INS; and

d) include a commitment to continual improvement of the INS management system.

The INS policy should:

a) be available as documented information;

b) be communicated within the organisation; and

c) be available to interested parties, as appropriate.

### 6.3 Roles, responsibilities within the organisation and authorities

Top management should ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated. Top management should assign the responsibilities and authority for:

a) ensuring that the INS management system conforms to the requirements of this guideline; and

b) reporting on the performance of the INS management system to top management.

NOTE: Top management may also assign responsibilities and authorities for reporting performance of the INS management system within the organisation.

These are the functions should be assigned in the applicable organisation:

a) regulatory/authority contact;

b) INS responsibility; and

c) risk management.

## 7. Support

### 7.1 Resources

The organisation should determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the INS management system.

### 7.2 Competence

The organisation should:

a) determine the necessary competence of person(s) doing work under its control that affects the performance of INS;

b) ensure that these persons are competent based on 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 i.e. the provision of training to, the mentoring of, or the re-assignment of current employees, or the hiring or contracting of competent persons.

### 7.3 Awareness

Persons doing work under the organisation's control should be aware of:

a) INS policy;

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

c) the implications of not conforming to the INS management system.

### 7.4 Communication

The organisation should determine the need for internal and external communications relevant to INS management system including:

a) what to communicate;

b) when to communicate;

c) with whom to communicate;

d) who should communicate; and

e) the process by which communication should be affected.

### 7.5 Documented information

#### 7.5.1 General

The organisation's INS management should include:

a) documented information required by this guideline; and

b) documented information determined by the organisation as being necessary for the effectiveness of the INS management system.

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

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

b) the complexity of processes and their interactions; and

c) the competence of the persons.

#### 7.5.2 Creating and updating

When creating and updating documented information the organisation should 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.

### 7.5.3 Control of documented information

Documented information required by the INS management system and by this guideline should 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 organisation should 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 organisation to be necessary for the planning and operation of the INS management system should 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.

## 8. Operations

### 8.1 Operational planning and control

The organisation should plan, implement and control the processes needed to meet INS requirements, and to implement the actions determined in 5.1. The organisation should also implement plans to achieve INS objectives determined in 6.2. The organisation should keep documented information to the extent necessary to have confidence that the processes have been carried out as planned. The organisation should control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary. The organisation should ensure that outsourced processes are determined and controlled.

## 9. Performance evaluation

### 9.1 Monitoring, measurement, analysis and evaluation

The organisation should evaluate the information security performance and the effectiveness of the INS management system. The organisation should determine the following items:

a) what needs to be monitored and measured, including INS 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 organisation should retain appropriate documented information as evidence of the monitoring and measurement results.

### 9.2 Internal audit

The organisation should conduct internal audits at planned intervals to provide information on whether the INS management system:

a) conforms to the organisation's own requirements for its INS management system and the requirements of this guideline; and

b) is effectively implemented and maintained.

The organisation should:

a) plan, establish, implement and maintain an audit program(s), including the frequency, method, responsibilities, planning requirements and reporting. The audit program(s) should 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 the objectivity and 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.

### 9.3 Management review

Top management should review the organisation's INS management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness. The management review should include considerations of:

a) the status of actions from previous management reviews;

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

c) feedback on the INS performance, including trends in:

   i) nonconformities and corrective actions;

   ii) monitoring and measurement results;

   iii) audit results; and

   iv) fulfilment of INS 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 should include decisions related to continual improvement opportunities and any needs for changes to the INS management system.

The organisation should retain documented information evidence of the results of management reviews.

## 10. Improvement

### 10.1 Nonconformity and corrective action

When nonconformity happens, the organisation should:

a) react to the nonconformity, and as applicable take action to control and correct it and 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 review the nonconformity, determining the causes of the nonconformity, and 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 INS management system, if necessary.

**Bibliography**

The following references are also recommended for the application of this guideline. For dated references, only the edition cited applies. For undated references, the latest edition of the references (including any amendments) applies.


[1] ISO/IEC 27001, Information technology - Security techniques - Information security management systems - Requirements.

[2] ISO/IEC 27002, Information technology - Security techniques - Code of practice for information security controls.

[3] ISO/IEC 27005, Information technology - Security technique - Information security risk management.

[4] NIST SP 800-37 Rev.2, Risk Management Framework for Information System and Organisations: A System Life Cycle Approach for Security and Privacy.

[5] NIST SP-800-39, Managing Information Security Risk: Organisation, Mission, and Information System View.

[6] [7] NIST SP-800-53, Security and Privacy Controls for Information Systems and Organisation, Revision 5.

[7] NIST SP 800-100, Information Security Handbook: A Guide for Managers.

[8] Centre for Internet Security (CIS), Critical Security Controls 20 V7.0.

[9] MCMC MTSFB TC G009:2019, Information and Network Security – Requirements

[10] Malaysian Personal Data Protection Act, 2010.

# Annex A
(normative)

## Controls

(Reference to applicable controls and how these controls can be applied)
The following controls [ITU-T X.1051| ISO/IEC 27011] apply based on identified risks in line with Section 5.2.6.

### A.1 Introduction

The list of controls is a combination of controls derives from Annex A of ISO 27001 and Critical Security Control CIS 20 V7.0. List of controls are divided into 4 categories as per Figure A.1.

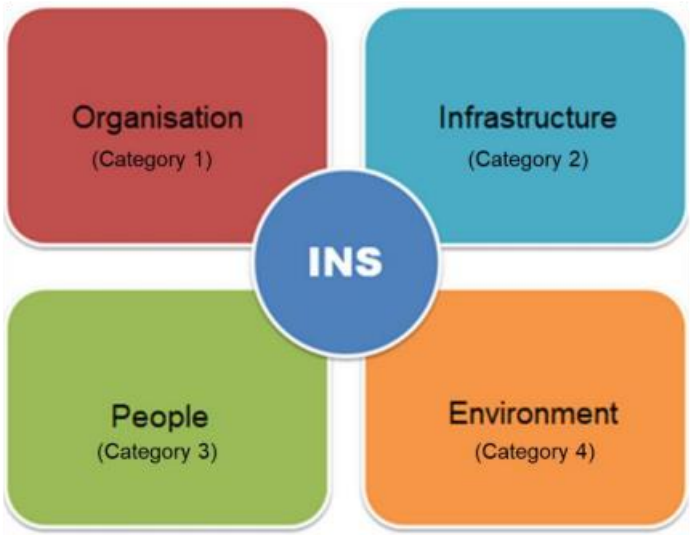


**Figure A.1. Families of control**

### A.2 Organisation (Category 1)

This family of control focuses on organisational readiness for INS. A business should have a formal and systematic approach to implementing and maintaining an effective INS program.

#### A.2.1 Information and Network Security (INS) policy

The organisation should develop 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.2.2 Business continuity management

Organisation survival depends on having a solid business continuity plan. This plan needs to incorporate the INS elements to ensure completeness and comprehensiveness of the plan, in line with the organisation's INS program. The plans are as follows:

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

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

c) information processing facilities should be implemented with redundancy sufficient to meet availability requirements.

### A.2.3 Information and Network Security (INS) compliance

Organisations are bound by the laws of the land, which requires compliance by identifying and understanding the legal, statutory, and contractual obligations pertaining to INS.

a) Applicable legal, statutory, and contractual obligations should be identified, documented and keep up to date.

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

c) Records/information, personal and sensitive data should be protected from loss, destruction, falsification, unauthorised access and unauthorised release, in accordance with legal, regulatory, contractual and business requirements.

d) Privacy and personally identifiable information should comply with relevant legislation and regulation where applicable.

e) The organisation's approach to managing INS and its implementation should be reviewed independently at planned intervals or when significant changes occur.

f) Information systems should be regularly reviewed for compliance with the organisation's INS policies, standards and any other security requirements.

### A.2.4 Organisation of information security

The organisation should establish the following management framework to initiate and control the implementation and operation of information security within the organisation:

a) information security roles and responsibilities;

b) segregation of duties;

c) contact with authorities;

d) contact with special interest groups; and
e) information security in project management.

The organisation also should establish a policy on mobile devices and teleworking.

### A.2.5 Information and Network Security (INS) incident management

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

The organisation should:

a) ensure that there are written incident response plans that defines roles of personnel as well as phases of incident handling/management;

b) establish procedures to ensure a quick, effective, and orderly response to security incidents;

c) designate management personnel, as well as backups, who will support the incident handling process by acting in key decision-making roles;

d) communicate security events and weaknesses in a manner allowing timely corrective action to be taken;

e) report incidents related to INS through appropriate management channels as quickly as possible;

f) properly collect, document and preserve evidence relating to a security violation;

g) properly investigate and analyse all incidents. Corrective action should be taken to recover from security violations. Subsequently, preventative measures should be taken to avoid the reoccurrence of the incident;

h) review preventative measures on a periodic basis (as part of operational procedural review) to evaluate the effectiveness of the controls and lessons learned; and

i) maintain third-party contact information to be used to report a security incident, such as Law Enforcement, relevant government departments, vendors and partners.

## A.3 Infrastructure (Category 2)

Managing the security of infrastructure of information security is one of the family of control focuses on organisational readiness for INS. This is due to growing information security risks, organisations should also continually monitor and effectively manage the security of their computing infrastructure to ensure the confidentiality, integrity, and availability of their information assets.

### A.3.1 Asset management

Business performance relies on its assets which may comprise of physical or virtual elements, network equipment, software, hardware and human capital. The organisation should ensure that:

a) all assets pertaining to information processing should be identified and maintained in an up-to-date inventory with the owners identified as well as their location;

b) in the case of hardware assets, the inventory should record the network address, machine name, category of asset, and asset owner and department for each asset;

c) these assets should be returned upon termination of employment, contract or agreement; and d) acceptable use of asset rules should be identified, documented and implemented.

### A.3.2 Data/Information management

To protect data/information, an organisation should perform as following controls.

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

b) Management of information lifecycle procedure should be implemented i.e. creating, processing, storing, distribution, destruction of information.

c) Test data should be carefully selected, protected and controlled.

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

### A.3.3 Media management

To prevent unauthorised disclosure, modifications, remover or destruction of information stored in a media, an organisation should perform the following.

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

b) Media containing information should be protected against unauthorised access, misuse or other damage.

c) Media intended to handle sensitive information should have functions for encryption or access control.

### A.3.4 Access control

To limit access to information and information processing facilities, an organisation should perform the following.

a) An access control policy should be drawn up, documented and reviewed based on business, information security and network security requirements.

b) Access to network and services should only be provided for those who have been specifically authorised.

### A.3.5 User access management

To ensure authorised user access and to prevent unauthorised access to systems and services, an organisation should perform the following.

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

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

c) The allocation of secret authentication information should be controlled through a formal management process.

d) Users should be required to adhere to organisation’s practices in the use and management of secret authentication information.

e) Allocation and use of privileged access rights should be restricted and controlled. Access should be granted or removed based on job roles and responsibility, adhering to the principle of least privilege and segregation of duties. Segregation of duties should be applied wherever feasible, according to business needs and requirements.

f) User and privilege access rights should be reviewed at regular intervals.

g) An inventory of all administrative accounts, including domain and local accounts should be maintained, to ensure that only authorised individuals have elevated privileges.

h) Before deploying any new asset, all default passwords should be changed to have values consistent with administrative level accounts.

i) All users with administrative account access should use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.

j) All authentication credentials should be encrypted or hashed when stored.

k) Any account that cannot be associated with a business process or business owner should be disabled.

l) Dormant accounts should be disabled after a set period of inactivity in accordance with the organisations policy.

### A.3.6 Systems, services and application access control

To prevent unauthorised access to systems, services and applications, an organisation should perform the following.

a) Access to systems, services and application should be restricted in accordance with the access control policy of the organisation.

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

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

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

e) Programmed source code access should be restricted.

f) Automatically lock workstation sessions after a standard period of inactivity.

### A.3.7 Cryptography

To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information, an organisation should perform the following.

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

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

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

d) Encrypt all sensitive information in storage, transit, and process.

e) Implement strong encryption in wireless data transmission.

### A.3.8 Information and Network (INS) in operations

To ensure correct and secure operations of information processing fatalities, an organisation should perform the following.

a) Documented security configuration standards and operating procedures should be maintained for all authorised network devices.

b) Changes made in the operations environment should be controlled, managed and documented.

c) Resources used in operations should be monitored, tuned and projections made of future capacity requirements to ensure required system performances are met.

d) Environments of development, testing and production should be kept separate to reduce risks of unauthorised access or changes.

e) All configuration rules that allow traffic to flow through network devices should be documented with a specific business reason.
f) The latest stable version of any security-related updates should be installed on all network devices.

g) The management network infrastructure should be managed separately from the business network infrastructure.

h) Regular scans should be performed from outside each trusted network boundary to detect any unauthorised connections which are accessible across the boundary.

i) Communications with known malicious or unused Internet IP addresses should be denied and access should be limited only to trusted and necessary IP address ranges at each of the organisation's network boundaries.

j) Communication over unauthorised Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) ports or application traffic should be denied to ensure that only authorised protocols are allowed to cross the network boundary in or out of the network at each of the organisation's network boundaries.

k) A separate wireless network for untrusted devices should be created.

### A.3.9 Malicious software protection

To ensure that information and information processing facilities are protected against malware, an organisation should perform the following.

a) Sufficient detection, prevention and recovery controls to protect against malware should be implemented.

b) Awareness on malware should be made to all organisation users.

c) The organisation's anti-malware software, scanning engine and signature database should be updated on a regular basis.

d) Devices should be configured so that they automatically conduct an anti-malware scan of removable media when inserted or connected.

e) All malware detection events should be logged to enterprise anti-malware administration tools and event log servers for analysis and alerting.

### A.3.10 Logging and monitoring

To record events and generate evidence, an organisation should perform the following.

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

b) Local logging should be enabled on all systems and networking devices.

c) Administrative and operator access should be logged and the logs regularly reviewed and sufficiently protected.

d) Systems should be configured to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.

e) System logging should be enabled to include detailed information such as event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

f) Appropriate logs should be stored for analysis and review. On a regular basis, logs should be reviewed to identify anomalies or abnormal events.

g) Logs and logging facilities should be protected against unauthorised access and tampering.

h) Clocks of all relevant systems/information and infrastructure should be synchronised to an organisation authorised reference time source.

i) All systems that store logs should have adequate storage space for the logs generated.

### A.3.11 Control of operational software

To ensure the integrity of operational systems, an organisation should perform the following.

a) Installation of software on operational system should be controlled based on installation and implementation procedures.

b) Documented security configuration should be maintained for authorised operating systems, databases and applications.

c) Secure images or templates for all systems in the enterprise should be maintained based on the organisation's approved configuration standards.

d) Only software that is approved by the organisation and properly licensed to the organisation should be added to the organisation's authorised software list.

### A.3.12 Technical vulnerability management

To prevent exploitation of technical vulnerabilities, an organisation should perform the following.

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

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

c) An up-to-date vulnerability scanning tool should be utilised to scan all systems on the network at least on a yearly or more frequent basis depending on the criticality of the business applications to identify all potential vulnerabilities on the organisation's systems.

d) The results from previous vulnerability scans should be compared with the current results to verify that vulnerabilities have been remediated in a timely manner.

e) A risk-rating process should be utilised to prioritise the remediation of discovered vulnerabilities.

### A.3.13 Information and network audit

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

### A.3.14 Backup

To protect against loss of data, an organisation should perform the following.

a) Backup of information, software and system should be performed in accordance to the backup policy.

b) Backup copies should be tested in accordance to the backup policy.

c) Backups should be properly protected via physical security or encryption when they are stored, as well as when they are moved across the network.

### A.3.15 Network communications security management

To ensure the protection of information in networks and its supporting information processing facilities, an organisation should perform the following.

a) Networks should be managed and controlled to protect information in systems, application and services.

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

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

d) Only network ports, protocols, and services listening on a system with validated business needs should be running on each system.

**A.3.16 Information transfer**

To maintain the security of information transferred within an organisation and with any external entity, an organisation should perform the following.

a) Formal policies, procedures and controls should be in place to protect information transfer through the use of all types of communication facilities. The organisation should minimally:

   i) block all e-mail attachments entering the organisation's e-mail gateway if the file types are unnecessary for the organisation's business; and

   ii) configure devices to not auto-run content from removable media.

b) Formal agreements should address the secure transfer of information between organisation and external parties.
c) Non-disclosure or confidentiality agreements reflecting the need of the organisation to protect information should be identified, regularly reviewed and documented.

d) Electronic messaging that contains any sensitive information of the organisation should be protected;

**A.3.17 Security requirements of systems**

To ensure that information security is an integral part of information systems across the entire lifecycle, an organisation should perform the following. This also includes the requirements for information systems which provide services over public networks.

a) INS related requirements should be included in the requirements for new systems or existing system enhancements.

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

c) Approved hardening configurations should be used for operating systems, databases and applications.

**A.3.18 Security requirements for development and support processes**

To ensure that information security is designed and implemented within the development lifecycle of information systems, an organisation should perform the following.

a) Procedures for development of systems, software and services should be established and applied to developments within the organisation.

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

c) Business critical applications, software and services should 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 should be strictly controlled; modifications to packages should be discouraged, limited to necessary changes.

e) Secure systems engineering principles should 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 should be drawn up.

g) Security functionality testing should be carried out during development.

h) Organisation should supervise and monitor activities of outsourced system development.

i) Acceptance testing criteria and programs should be established for new systems, upgrades and new versions.

**A.3.19 System acquisition, development and maintenance**

To ensure protection of information during system acquisition, development and maintenance, an organisation should do the following:

a) All security requirements should be identified and analysed 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.

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

c) Establish secure coding practices, e.g., Open Web Application Security Project (OWASP), appropriate to the programming language and development environment being used.

d) Verify that the version of all software acquired from outside your organisation is still supported by the developer.

e) Use only standardised encryption algorithms for development.

f) For applications that rely on a database, use standard hardening configuration templates.

## A.4 People (Category 3)

Although technology is an essential part of the process of securing information assets, it is the people responsible for design, implementation and operation of these technological tools that may be driving or restraining forces in the effective implementation of the management system.

### A.4.1 Human resource security

To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered, which include:

a) The organisation should ensure employees and contractors understand and comply with their responsibilities and are suitable for the roles for which they are assigned.

b) The organisation should 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.

c) The organisation should ensure that the organisation's security awareness program is reviewed at least annually to address new technologies, threats, standards and business requirements.

### A.4.2 Supplier relationships

To ensure protection of the organisation’s assets that is accessible by suppliers, an organisation should perform the following.

a) The organisation should 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 should include requirements for INS and address INS risks associated with information technology services and product supply chain.

c) Organisation should regularly monitor, review, audit supplier service delivery.

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

## A.5 Environment (Category 4)

Physical and environmental security is an essential factor in protecting people, data, equipment, systems, facilities and company asset. The information security and physical and environmental security need to work conjointly in achieving and maintaining confidentiality, integrity and availability of information, and information processing facilities, including telecommunication systems and infrastructure, and to protect against cyber-crime, fraudulent activities, information loss and other security risks and threats.

### A.5.1 Physical and environmental security

To prevent unauthorised physical access, damage and interference to the organisation's information and information processing facilities, an organisation should ensure the following.

a) The organisation should ensure that physical and environmental security controls are identified, and these controls are implemented.

b) Physical and environmental security measures should prevent unauthorised physical access, damage and interference to the organisation's premises and information.

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

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

e) All items of equipment containing storage media should 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)

## CSIRT and SOC

Organization may also consider the establishment of organizational CSIRT and Security Operation Centre (SOC) to continuously monitor and mitigate security risks, threats, and vulnerabilities.

_____