HONG KONG INTERNET REGISTRATION CORPORATION LTD.

HONG KONG DOMAIN NAME REGISTRATION COMPANY LTD.

INFORMATION SECURITY POLICY

Document id: P01

Version 2.6.1

29 AUG 2025

Note: © **Hong Kong Internet Registration Corporation Ltd.** The contents of this document remain the property of and may not be reproduced in whole or in part without the express permission of the **Hong Kong Internet Registration Corporation Ltd**.

Document Control

Document Owner	Classification	Publication Date
ISMC	UNCLASSIFIED	29 AUG 2025

Document Version

Version No	Revision Date	Summary of Changes
1.00	2007-12-06	Initial release and approval
1.01	2016-08-05	Update company logo and expiry date
2.0	2019-01-09	Update content in alignment with the requirements of ISO 27001:2013
2.1	2020-06-05	Annual review - No Change
2.2	2021-07-11	Annual review - No Change
2.3	2022-06-02	Annual review - No Change
2.4	2023-06-28	Annual review - No Change
2.5	2024-04-30	Update content in alignment with the requirements of ISO 27001:2022
2.6	2024-08-15	Update content in alignment with the requirements of ISO 27001:2022
2.6.1	2025-08-29	Annual review - Revised

Document Distribution

Copy	Issued To	Location
Master	ISMC	Intranet File Server

TABLE OF CONTENT

1. PURPOSE 1

2. SCOPE 2

3. REFERENCE AND DEFINITIONS 3

3.1 STANDARDS AND GUIDELINES 3
3.2 TERMS AND DEFINITIONS 3

4. CONVENTIONS 5

5. RISK ASSESSMENT, AUDIT AND MANAGEMENT REVIEW 6

5.1 RISK ASSESSMENT 6
5.2 AUDIT 6
5.3 MANAGEMENT REVIEW OF THE ISMS 6
5.4 ISMS IMPROVEMENT 7

6. ORGANIZATION OF INFORMATION SECURITY 8

6.1 SENIOR MANAGEMENT 9
6.2 INFORMATION SECURITY MANAGEMENT COMMITTEE (ISMC) 9
6.3 INFORMATION SECURITY OFFICER (ISO) 10
6.4 INFORMATION SECURITY INCIDENT RESPONSE TEAM (ISIRT) COMMANDER 10
6.5 INFORMATION SECURITY ADMINISTRATORS 11
6.6 INFORMATION OWNERS 11
6.7 NETWORK / SYSTEM ADMINISTRATORS 12
6.8 APPLICATION DEVELOPMENT & MAINTENANCE TEAM 12
6.9 USERS OF INFORMATION SYSTEMS 12

7. HUMAN RESOURCES SECURITY 13

7.1 PRIOR TO EMPLOYMENT 13
7.2 DURING EMPLOYMENT 13
7.3 TERMINATION AND CHANGE OF EMPLOYMENT 13

8. ASSET MANAGEMENT 14

8.1 RESPONSIBILITY FOR ASSETS 14
8.2 INFORMATION CLASSIFICATION 14
8.3 MEDIA HANDLING 14

9. ACCESS CONTROL 15

9.1 BUSINESS REQUIREMENT OF ACCESS CONTROL 15
9.2 USER ACCESS MANAGEMENT 15
9.3 USER RESPONSIBILITIES 16
9.4 NETWORK ACCESS CONTROL 16
9.5 OPERATING SYSTEM ACCESS CONTROL 16
9.6 APPLICATION AND INFORMATION ACCESS CONTROL 17
9.7 MOBILE DEVICES AND TELEWORKING 17

10. CRYPTOGRAPHIC CONTROL 19

10.1 CRYPTOGRAPHIC CONTROLS 19

11. PHYSICAL AND ENVIRONMENTAL SECURITY 19

11.1 SECURE AREAS 19
11.2 EQUIPMENT SECURITY 20

12. OPERATIONS SECURITY 20
12.1 OPERATIONAL PROCEDURES AND RESPONSIBILITIES 20
12.2 PROTECTION FROM MALWARE 21
12.3 BACKUP 21
12.4 LOGGING AND MONITORING 21
12.5 CONTROL OF OPERATIONAL SOFTWARE 21
12.6.1.1 TECHNICAL VULNERABILITY MANAGEMENT 22
12.7 INFORMATION SYSTEMS AUDIT CONSIDERATIONS 22
13. COMMUNICATIONS SECURITY 23
13.1 NETWORK SECURITY MANAGEMENT 23
13.2 INFORMATION TRANSFER 23
14. SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE 24
14.1 SECURITY REQUIREMENTS OF INFORMATION SYSTEMS 24
14.2 SECURITY IN DEVELOPMENT AND SUPPORT PROCESS 24
14.3 TEST DATA 25
15. SUPPLIER RELATIONSHIP 25
15.1 INFORMATION SECURITY IN SUPPLIER RELATIONSHIPS 25
15.2 SUPPLIER SERVICE DELIVERY MANAGEMENT 25
16. INFORMATION SECURITY INCIDENT MANAGEMENT 26
16.1 MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS 26
17. INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT 26
17.1 INFORMATION SECURITY CONTINUITY 26
17.2 REDUNDANCIES 27
18. COMPLIANCE 27
18.1 COMPLIANCE WITH LEGAL AND CONTRACTUAL REQUIREMENTS 27
18.2 INFORMATION SECURITY REVIEWS 28

1. PURPOSE

Hong Kong Internet Registration Corporation Limited / Hong Kong Domain Name Registration Company Limited (hereafter referred as the "Organization") shall establish, implement, operate, monitor, review, maintain and improve a documented Information Security Management System (ISMS) within the context of the Organization's overall business activities and the risks it faces.

This document constitutes an Information Technology (IT) Security Policy that interested internal and external parties of the Organization shall observe and follow. For the purposes of this Policy the process used is based on the PDCA model shown in FIGURE 1.

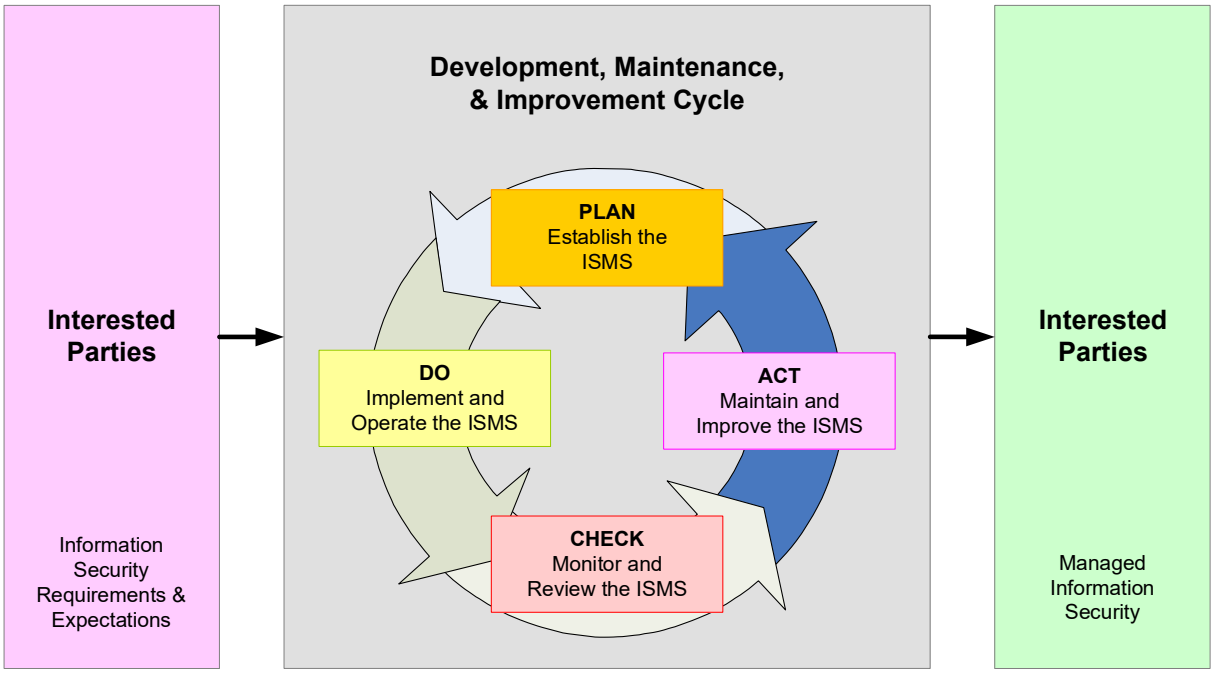


FIGURE 1 – PDCA Model Applied to ISMS processes

PLAN (establish the ISMS) - Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with the Organization's overall policies and objectives.

DO (implement and operate the ISMS) - Implement and operate the ISMS policy, controls, processes and procedures.

CHECK (monitor and review the ISMS) - Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.

ACT (maintain and improve the ISMS) - Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.

The process approach for information security management in this Policy encourages its users to emphasize the importance of:

(a) understanding the Organization's information security requirements and the need to establish policy and objectives for information security;

(b) implementing and operating controls to manage the Organization's information security risks in the context of the Organization's overall business risks;

(c) monitoring and reviewing the performance and effectiveness of the ISMS; and

(d) continual improvement based on objective measurement.

2. SCOPE

This document addresses security considerations in the following areas:

(a) Risk Assessment and Treatment

(b) Organization of Information Security

(c) Management Responsibilities

(d) Human Resources Security

(e) Asset Management

(f) Access Control

(g) Cryptographic Control

(h) Physical and Environmental Security

(i) Operations Security

(j) Communications Security

(k) Systems Acquisition, Development and Maintenance

(l) Supplier Relationship

(m) Information Security Incident Management

(n) Business Continuity Management

(o) Compliance

3. REFERENCE AND DEFINITIONS

3.1 STANDARDS AND GUIDELINES

(a) ISO27001:2022 "Information security, cybersecurity and privacy protection – Information security management systems – Requirements"

(b) ISO27002:2022 "Information security, cybersecurity and privacy protection – Information security controls"

3.2 TERMS AND DEFINITIONS

(a)	Asset	Anything that has value to the Organization.
(b)	Asset Owner	The term 'asset owner' identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. The term 'asset owner' does not mean that the person actually has property rights to the asset.
(c)	Availability	The property of being accessible and usable upon demand by an authorized entity.
(d)	Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
(e)	Information system	A related set of hardware and software organised for the collection, processing, storage, communication, or disposition of information.
(f)	Information security	Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.
(g)	Information security event	An identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.
(h)	Information security incident	A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

(i)	Information security management system (ISMS)	Part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security. NOTE: The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.
(j)	Integrity	The property of safeguarding the accuracy and completeness of assets.
(k)	Malware	Programs intended to perform an unauthorised process that will have an adverse impact on the confidentiality, integrity, or availability of an information system. Examples of malware include computer viruses, worms, Trojan horses, and spyware etc.
(l)	Mobile Devices	Portable computing and communication devices with information storage and processing capability. Examples include portable computers, mobile phones, tablets, digital cameras, and audio or video recording devices.
(m)	Removable Media	Portable electronic storage media such as magnetic, optical, and flash memory devices, which can be inserted into and removed from a computing device. Examples include external hard disks or solid-state drives, floppy disks, zip disks, optical disks, tapes, memory cards, flash drives, and similar USB storage devices.
(n)	Residual risk	The risk remaining after risk treatment.
(o)	Risk acceptance	Decision to accept a risk.
(p)	Risk analysis	Systematic use of information to identify sources and to estimate the risk.
(q)	Risk assessment	Overall process of risk identification, risk analysis and risk evaluation.
(r)	Risk evaluation	Process of comparing the estimated risk against given risk criteria to determine the significance of the risk.
(s)	Risk management	Coordinated activities to direct and control an organization with regard to risk.

(t) Risk treatment — Process of selection and implementation of measures to modify risk.

4. CONVENTIONS

The following is a list of conventions used in this document:

Shall	the use of the word 'shall' indicates a mandatory requirement.
Should	the use of the word 'should' indicates a requirement for good practice, which should be implemented whenever possible.
May	the use of the word 'may' indicates a desirable requirement.

5. RISK ASSESSMENT, AUDIT AND MANAGEMENT REVIEW

5.1 RISK ASSESSMENT

5.1.1 A risk assessment methodology that is suited to the Information Security Management System, and the identified business information security, legal and regulatory requirements, shall be developed.

5.1.2 Criteria for accepting risk shall be developed to identify acceptable levels of risk, and risk assessment shall be conducted to determine whether the risks are acceptable or require treatment.

5.1.3 Risk assessment shall be conducted periodically; prior to development, major enhancements and changes associated with the systems or applications.

5.1.4 The Organization shall identify changed risks and identify preventive action requirements focusing attention on significantly changed risks. The priority of preventive actions shall be determined based on the results of the risk assessment.

5.2 AUDIT

5.2.1 Audit shall be conducted at planned intervals to determine whether controls objectives, controls, processes and procedures of its Information Security Management System:

(a) conform to the identified information security requirements;

(b) are effectively implemented and maintained; and

(c) performed as expected.

5.2.2 An audit programme shall be planned, taking into consideration the status and importance of the processes and areas to be audited, as well as the results of previous audits. The audit criteria, scope, frequency and methods shall be defined.

5.2.3 The selection of auditors and conduct of audits shall ensure objectivity and impartiality of the audit process. Auditors shall not audit their own work.

5.2.4 The management responsible for the area being audited shall ensure that actions are taken without undue delay to eliminate detected nonconformities and their causes. Follow-up activities shall include the verification of the actions taken and the reporting of verification results.

5.3 MANAGEMENT REVIEW OF THE ISMS

5.3.1 Management shall review the Organization’s ISMS at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

5.3.2 Management review shall include assessing opportunities for improvement and the need for changes to the ISMS, including the information security policy and information security objectives. The results of the reviews shall be clearly documented and records shall be maintained.

5.4 ISMS IMPROVEMENT

5.4.1 The Organization shall continually improve the effectiveness of the ISMS through the use of the information security policy, information security objectives, audit results, analysis of monitored events, corrective and preventive actions and management review.

5.4.2 The Organization shall determine and take action to eliminate the cause of nonconformities with the ISMS requirements in order to prevent recurrence. Preventive actions taken shall be appropriate to the impact of the potential problems.

6. ORGANIZATION OF INFORMATION SECURITY

Security objective: To establish a framework for the management of information security within the Organization to initiate and control the implementation of information security within the Organization.

The following diagram describes the IT security organizational framework of the Organization:

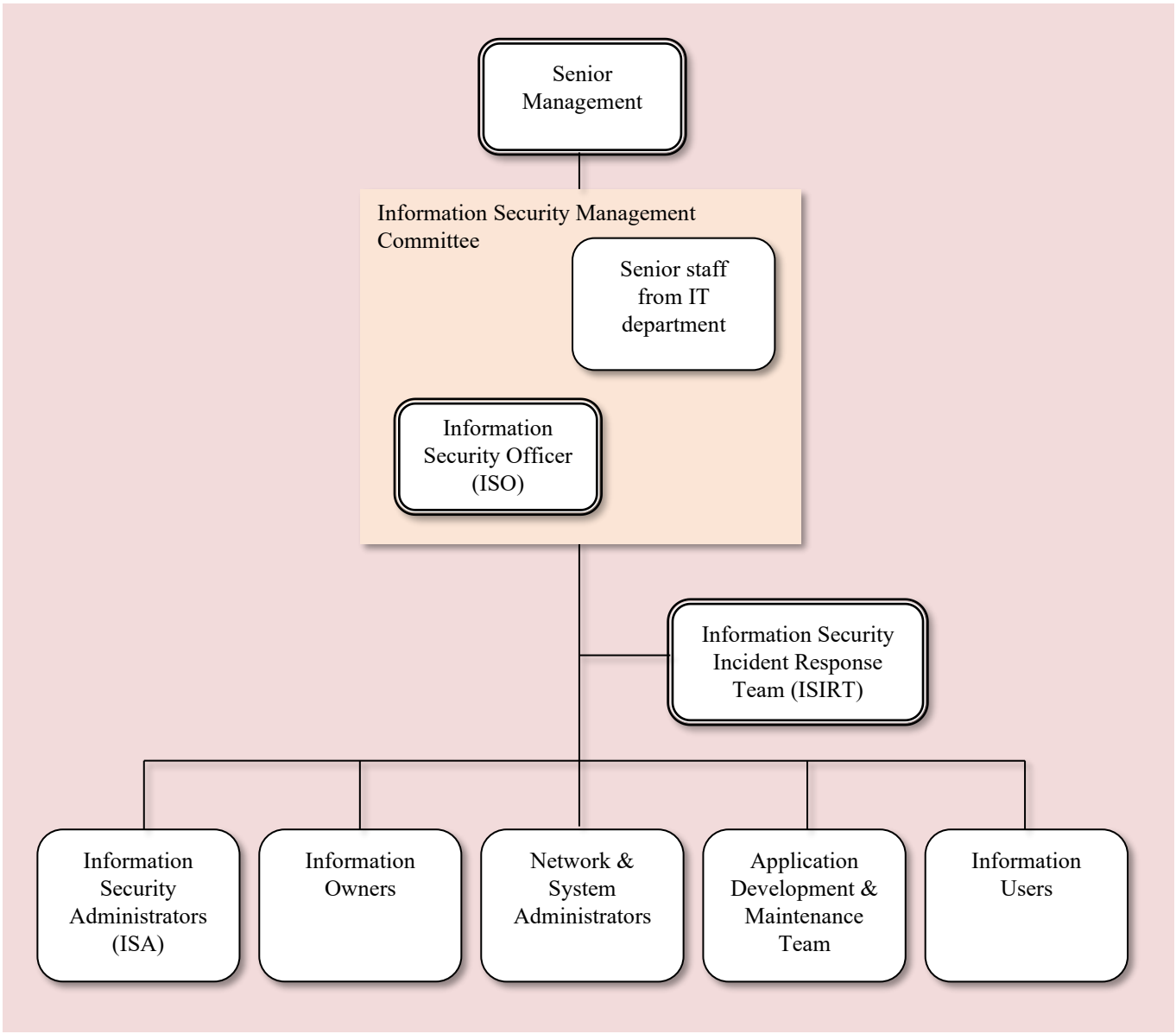


FIGURE 2 – Organization Chart for ISMS

6.1 SENIOR MANAGEMENT

Senior management shall commit to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS by:

(a) establishing, implementing, monitoring and continuously improving an ISMS and related policy;
(b) ensuring the information security policy and the information security objectives are established and are compatible with the Organization's strategic direction;
(c) ensuring the integration of ISMS requirements into business processes and life cycle activities;
(d) communicating to the related stakeholders on the importance of effective information security management, conforming to the information security policy, and satisfying applicable business, customer, legal, regulatory, and contractual requirements related to information security;
(e) ensuring that ISMS achieves the intended outcomes;
(f) providing sufficient resources, including manpower, infrastructure, hardware, software to establish, implement, monitor, review, maintain and improve the ISMS;
(g) directing and supporting persons to contribute to the effectiveness of ISMS;
(h) promoting continual improvement;
(i) supporting other relevant management roles to demonstrate the leadership as it applies to their areas of responsibility;
(j) ensuring the risk management process is in place, and the residual risk is continuously reduced to an acceptable level; and
(k) ensuring the internal audits and management reviews are conducted, the results are reviewed, and relevant actions and safeguard are implemented to reduce the overall impacts and risks.

6.2 INFORMATION SECURITY MANAGEMENT COMMITTEE (ISMC)

The Organization shall establish an Information Security Management Committee (ISMC) to oversee the IT security within the whole Organization. The committee meets on a regular basis to:

(a) Review and endorse changes to the IT security related policies;
(b) Review and endorse the criteria for accepting risks and the acceptable levels of risk;
(c) Define specific roles and responsibilities relating to IT security; and
(d) Provide guidance and assistance to departments in the enforcement of IT security related policies.

The core members of ISMC comprise representatives from:

(a) Senior staff(s) from IT departments.

(b) Information Security Officer.

Representative(s) from other departments will be co-opted into the Committee on a need basis, in relation to specific subject matters.

6.3 INFORMATION SECURITY OFFICER (ISO)

The Organization shall appoint Information Security Officer (ISO) to be responsible for IT security. The roles and responsibilities of ISO shall be clearly defined which include but are not limited to the following:

(a) Implement, operate and maintain the ISMS;

(b) Ensure that activities are performed to identify, document and fulfil information security requirements;

(c) Develop and modify information security policies, standards, procedures and guidelines

(d) Ensure that risk assessment is conducted periodically & monitor changed risks

(e) Ensure that appropriate security control objectives and measures are selected and implemented;

(f) Monitor compliance to security standards, and conduct regular reviews;

(g) Schedule security awareness training and ensure training effectiveness;

(h) Liaise with external parties on matters related to the internal and external communication;

(i) Implement corrective and preventive recommendations from security reviews or audits;

(j) Organize ISMC meetings; report on the performance and opportunities for improvement to the ISMS;

(k) Maintain appropriate contacts with relevant authorities; and

(l) Maintain appropriate contacts with special interest groups or other specialist security forums and professional associations.

6.4 INFORMATION SECURITY INCIDENT RESPONSE TEAM (ISIRT) COMMANDER

The ISIRT is the central focal point for coordinating the handling of information security incidents occurring within the Organization. The Management should designate an officer from the senior management to be the ISIRT Commander. The ISIRT Commander should

have the authority to appoint core team members for the ISIRT. The responsibilities of an ISIRT Commander include:

(a) Provide overall supervision and co-ordination of information security incident handling for all Information Systems within the Organization;

(b) Make decisions on critical matters such as system recovery, the engagement of external parties and the extent of involvement, and service resumption logistics after recovery etc.;

(c) Trigger the disaster recovery procedure where appropriate, depending on the impact of the incident on the business operation of the ;

(d) Provide management endorsement on the provision of resources for the incident handling process;

(e) Provide management endorsement in respect of the line-to-take for publicity on the incident;

(f) Facilitate experience and information sharing within the Organization on information security incident handling and related matters.

6.5 INFORMATION SECURITY ADMINISTRATORS

Information Security Administrators are responsible for providing security and risk management related support services. They assist in identifying system vulnerabilities and performing security administrative work of the system. His / her responsibilities also include:

(a) Review control and access to the system;

(b) Check and manage audit logs; and

(c) Review user accounts;

The Information Security Administrator may or may not be a technical person, but he/she should not be the same person as the Network / System Administrator. There should be segregation of duties between the Information Security Administrator and the Network / System Administrator.

6.6 INFORMATION OWNERS

Information Owners are the collators and the owners of information stored in databases and data files. Their primary responsibility is to:

(a) Determine the security requirements and security classifications, usage and protection of the information; and

(b) **This requirement is mandatory to the IT Department only; other departments are recommended to follow where possible.**

Ensure that information security is addressed in project management regardless of the type of the project.

6.7 NETWORK / SYSTEM ADMINISTRATORS

Network / System Administrators are responsible for the day-to-day administration, operation and configuration of the computer systems and network in , whereas Internet System Administrators are responsible for the related tasks for their Internet-facing Information Systems. Their responsibilities include:

(a) Implement the security mechanisms in accordance with procedures/guidelines established by the Information Security Officer;

(b) Maintain control and access to the system; and

(c) Maintain user account.

6.8 APPLICATION DEVELOPMENT & MAINTENANCE TEAM

The Application Development & Maintenance Team is responsible for producing the quality systems in the use of quality procedures, techniques and tools. Their responsibilities include:

(a) Liaise with the Information Owner in order to agree on system security requirements; and

(b) Define the solutions to implement these security requirements.

6.9 USERS OF INFORMATION SYSTEMS

Users of Information Systems are the staff who actually use the information and shall be accountable for all their activities on the Information Systems. Responsibilities of an information system user include:

(a) Know, understand, follow and apply all the possible and available security mechanisms to the maximum extent possible; and

(b) Prevent unauthorized access to their computers and workstations at his/her best effort.

7. HUMAN RESOURCES SECURITY

7.1 PRIOR TO EMPLOYMENT

Security objective: To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.

7.1.1 Security roles and responsibilities of employees, contractors and third party users shall be defined and documented in accordance with the Organization's information security policy.

7.1.2 Background verification checks on all candidates for employment, contractors, and third party users shall be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

7.1.3 As part of their contractual obligation, employees, contractors and third party users shall agree and sign the terms and conditions of their employment contract, which shall state their and the Organization's responsibilities for information security.

7.2 DURING EMPLOYMENT

Security objective: To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.

7.2.1 Management shall require employees, contractors and third party users to apply security in accordance with established policies and procedures of the Organization.

7.2.2 All employees of the Organization and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.

7.2.3 There shall be a formal disciplinary process for employees who have committed a security breach.

7.3 TERMINATION AND CHANGE OF EMPLOYMENT

Security objective: To ensure that employees, contractors and third party users exit the Organization or change employment in an orderly manner.

7.3.1 Responsibilities for performing employment termination or change of employment shall be clearly defined and assigned.

7.3.2 All employees, contractors and third party users shall return all of the Organization's assets in their possession upon termination of their employment, contract or agreement.

7.3.3 The access rights of all employees, contractors and third party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

7.3.4 Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.

8. ASSET MANAGEMENT

8.1 RESPONSIBILITY FOR ASSETS

Security objective: To achieve and maintain appropriate protection of organizational assets.

8.1.1 All assets shall be clearly identified and an inventory of all important assets drawn up and maintained.

8.1.2 All information and assets associated with information processing facilities shall be 'owned' by a designated part of the Organization.

8.1.3 Organization provided electronic communication systems solely to facilitate business purposes and communications, and are only to be used for management-approved activities. These systems, including the equipment and the data stored in the system, are and remain the property of the Organization.

8.2 INFORMATION CLASSIFICATION

Security objective: To ensure that information receives an appropriate level of protection.

8.2.1 Information shall be classified in terms of its legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.

8.2.2 An appropriate set of procedures for information labelling and handling shall be developed and implemented in accordance with the *Information Security Classification Policy*.

8.2.3 **This requirement is mandatory to the IT Department only; other departments are recommended to follow where possible.**

Staff shall not store classified information on non-company subscribed cloud services.

8.3 MEDIA HANDLING

Security objective: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

8.3.1 There shall be procedures in place for the management of removable media.

8.3.2 Media shall be disposed of securely and safely when no longer required, using formal procedures.

8.3.3 Procedures for the handling and storage of information shall be established to protect this information from unauthorized disclosure or misuse.

8.3.4 Media containing information shall be protected against unauthorized access, misuse or corruption during transportation beyond the Organization's physical boundaries.

8.3.5 System documentation shall be protected against unauthorized access.

9. ACCESS CONTROL

9.1 BUSINESS REQUIREMENT OF ACCESS CONTROL

Security objective: To control access to information.

9.1.1 Access to network, systems, applications and information are granted to users on a need-to-know basis, taking into considerations of the business need versus security implications, separation of duties within business processes, and classification of information.

9.1.2 For network connectivity or services, the security principle "Everything is generally forbidden unless expressly permitted" shall also be considered when granting accesses.

9.2 USER ACCESS MANAGEMENT

Security objective: To ensure authorized user access and to prevent unauthorized access to information systems.

9.2.1 There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.

9.2.2 The allocation and use of privileged access rights shall be restricted and controlled.

9.2.3 Administrative or privileged access rights shall be given to limited number of staff and their activities should be logged and reviewed. Authorization to individual users or request for administrative privileges should be prohibited.

9.2.4 The allocation of secret authentication information shall be controlled through a formal management process.

9.2.5 Management shall review users' access rights at regular intervals using a formal process.

9.3 USER RESPONSIBILITIES

Security objective: To prevent unauthorized user access, and compromise or theft of information and information processing facilities.

9.3.1 Users shall be required to follow good security practices in the selection and use of passwords.

9.3.2 Users shall ensure that unattended equipment has appropriate protection.

9.3.3 Users shall follow the clear desk requirements for papers and removable storage media and the clear screen requirements for information processing.

9.4 NETWORK ACCESS CONTROL

Security objective: To prevent unauthorized access to networked services.

9.4.1 Users shall only be provided with access to the services that they have been specifically authorized to use.

9.4.2 Appropriate authentication methods shall be used to control access by remote users.

9.4.3 Automatic equipment identification shall be considered as a means to authenticate connections from specific locations and equipment.

9.4.4 Physical and logical access to diagnostic and configuration ports shall be controlled.

9.4.5 For shared networks, especially those extending across the Organization's boundaries, the capability of users to connect to the network shall be restricted, in line with the access control policy and requirements of the business applications.

9.4.6 Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.

9.5 OPERATING SYSTEM ACCESS CONTROL

Security objective: To prevent unauthorized access to operating systems.

9.5.1 Access to operating systems shall be controlled by a secure log-on procedure.

9.5.2 All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.

9.5.3 Systems for managing passwords shall be interactive and shall ensure quality passwords.

9.5.4 The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.

9.5.5 Inactive sessions shall shut down after a defined period of inactivity.

9.5.6 Restrictions on connection times shall be used to provide additional security for high-risk applications.

9.5.7 Access to program source code shall be restricted.

9.6 APPLICATION AND INFORMATION ACCESS CONTROL

Security objective: To prevent unauthorized access to information held in application systems.

9.6.1 Access to information and application system functions by users and support personnel shall be restricted in accordance with the defined access control policy.

9.6.2 Where feasible, data masking techniques shall be employed to obscure sensitive data, thereby minimizing risk of unintended disclosure.

9.6.3 Sensitive systems shall have a dedicated (isolated) computing environment.

9.7 MOBILE DEVICES AND TELEWORKING

Security objective: To ensure the security of teleworking and use of mobile devices.

9.7.1 **This requirement is mandatory to the IT Department only; other departments are recommended to follow where possible.**

Before using privately owned mobile devices to access company internal network, data and systems, staff shall acknowledge their responsibilities specified in this policy and obtain approval from Information Security Officer.

9.7.2 **This requirement is mandatory to the IT Department only; other departments are recommended to follow where possible.**

Smartphones / tablet computers shall not be jail-broken, rooted or have any software / firmware installed which is designed to gain access to functionality not intended to be exposed to users. Mobile devices should be kept up to date with manufacturer / developer provided patches.

9.7.3 **This requirement is mandatory to the IT Department only; other departments are recommended to follow where possible.**

Applications shall only be installed from official platform-owner approved sources. Installation of code from un-trusted sources is forbidden.

9.7.4 Suitable and up-to-date firewall and virus protection software should be installed on the notebook computers at all times.

9.7.5 **This requirement is mandatory to the IT Department only; other departments are recommended to follow where possible.**

Mobile devices shall not be connected to any computer which does not have up-to-date and enabled anti-malware protection.

9.7.6 The organization reserves the right to remote wiping the information or content stored on the company provided smartphones / tablet computers.

9.7.7 **This requirement is mandatory to the IT Department only; other departments are recommended to follow where possible.**

It is the responsibility of all remote access users to ensure that the remote access connection is given the same consideration as the user's onsite connection from within the organization.

9.7.8 **This requirement is mandatory to the IT Department only; other departments are recommended to follow where possible.**

Reconfiguration of user equipment for the purpose of split-tunnelling or dual homing should not be permitted during remote access connections.

9.7.9 **This requirement is mandatory to the IT Department only; other departments are recommended to follow where possible.**

Computer equipment used for remote access to the organization’s networks should have latest security patches and suitable endpoint security solution (i.e. personal firewall and antivirus software) with the latest virus definition file installed.

9.7.10 **This requirement is mandatory to the IT Department only; other departments are recommended to follow where possible.**

Suitable quarantine controls should be deployed to inspect the security patch levels and virus definition file date of the computer equipment before the accepting remote access connection request by the remote access server.

10. CRYPTOGRAPHIC CONTROL

10.1 CRYPTOGRAPHIC CONTROLS

Security Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

10.1.1 Proven and standard algorithms shall be used as the basis for encryption technologies.

10.1.2 Asymmetric cryptosystem keys shall be of a length that yields equivalent strength as stated in the *Information Security Standard*. Cryptographic key length requirements will be reviewed annually and upgraded as technology advances.

10.1.3 The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts independent of the provider and approved by the Information Security Officer.

10.1.4 The export and uses of encryption technologies is restricted in some countries. Staff should make themselves aware of the encryption technology laws of the country in which they reside.

10.1.5 Key management shall be in place to support the Organization's use of cryptographic techniques.

11. PHYSICAL AND ENVIRONMENTAL SECURITY

11.1 SECURE AREAS

Security objective: To prevent unauthorized physical access, damage and interference to the Organization's premises and information.

11.1.1 Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) shall be used to protect areas that contain information and information processing facilities.

11.1.2 Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

11.1.3 Physical security for offices, rooms, and facilities shall be designed and applied.

11.1.4 Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster shall be designed and applied.

11.1.5 Physical protection and guidelines for working in secure areas shall be designed and applied.

11.1.6 Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

11.2 EQUIPMENT SECURITY

Security objective: To prevent loss, damage, theft or compromise of assets and interruption to the Organization's activities.

11.2.1 Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

11.2.2 Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.

11.2.3 Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.

11.2.4 Equipment shall be correctly maintained to ensure its continued availability and integrity.

11.2.5 Security shall be applied to off-site equipment taking into account the different risks of working outside the Organization's premises.

11.2.6 All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.

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

12. OPERATIONS SECURITY

12.1 OPERATIONAL PROCEDURES AND RESPONSIBILITIES

Security objective: To ensure the correct and secure operation of information processing facilities.

12.1.1 Operating procedures shall be documented, maintained, and made available to all users who need them.

12.1.2 Changes to information processing facilities and systems shall be controlled.

12.1.3 Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the Organization's assets.

12.1.4 The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.

12.1.5 Development, test and operational facilities shall be separated to reduce the risks of unauthorised access or changes to the operational system.

12.2 PROTECTION FROM MALWARE

Security objective: To ensure that information and information processing facilities are protected against malware.

12.2.1 Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented.

12.3 BACKUP

Security objective: To protect against loss of data.

12.3.1 Backup copies of information and software shall be taken and tested regularly in accordance with the agreed backup policy.

12.4 LOGGING AND MONITORING

Security objective: To record events and generate evidence.

12.4.1 Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.

12.4.2 Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly.

12.4.3 Logging facilities and log information shall be protected against tampering and unauthorized access.

12.4.4 System administrator and system operator activities shall be logged.

12.4.5 Faults shall be logged, analyzed, and appropriate action taken.

12.4.6 The clocks of all relevant information processing systems within the Organization or security domain shall be synchronized with an agreed accurate time source.

12.5 CONTROL OF OPERATIONAL SOFTWARE

Security objective: To ensure the integrity of operational systems.

12.5.1 Procedures shall be implemented to control the installation of software on operational systems.

12.6 TECHNICAL VULNERABILITY MANAGEMENT

Security objective: To prevent exploitation of technical vulnerabilities.

12.6.1 Timely information about technical vulnerabilities of information systems being used shall be obtained, the Organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

12.6.2 Upon receiving security vulnerability alerts or patch related information, an evaluation of the security vulnerability should be conducted by Information Security Officer, taking into consideration of the existing network and system protection, to confirm the existence of vulnerability in hardware and software, and determine the priority of patch installation.

12.6.3 Upon receiving the end-of-life or end-of-support announcement from vendor, a technology refreshment plan should be established to replace / upgrade the affected hardware and/or software. An evaluation should be conducted for systems approaching end-of-support dates to assess risks of continued usage. Effective security controls should be established accordingly.

12.6.4 If patch installation on a network equipment, server or application or replacing / upgrading it is not feasible, suitable compensating controls (for example, intrusion preventive / detection mechanism, restrictive firewall filtering) should be implemented to minimize the risk of vulnerability exploitation.

12.6.5 If granted administrative privileges, staff shall only install work related software to the computers or network devices. Staff shall not install software with potentially or suspected malicious origin / behaviour, or software for personal use. Installation of software by non-administrative users is prohibited.

12.7 INFORMATION SYSTEMS AUDIT CONSIDERATIONS

Security objective: To minimise the impact of audit activities on operational systems.

12.7.1 Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.

12.7.2 Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.

13. COMMUNICATIONS SECURITY

13.1 NETWORK SECURITY MANAGEMENT

Security objective: To ensure the protection of information in networks and its supporting information processing facilities.

13.1.1 Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.

13.1.2 Security mechanisms, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.

13.1.3 Groups of information services, users, and information systems shall be segregated on networks.

13.2 INFORMATION TRANSFER

Security objective: To maintain the security of information transferred within the Organization and with any external entity.

13.2.1 Appropriate password protection or data encryption shall be used in transmitting classified information to external parties over electronic communication systems.

13.2.2 Staff should aware that contents of electronic communications may be maintained, stored and read by the Organization as deemed necessary. Deletion does not insure permanent removal, it may still be possible to recover the message; therefore, the ultimate privacy of message may not be assured.

13.2.3 Electronic communication messages shall not be created or sent which may constitute intimidating, hostile, or offensive material on the basis of race, colour, creed, religion, national origin, age, sex, marital status, lawful alien status, non-job-related physical or mental disability, veteran status, sexual orientation, or other basis prohibited by law.

13.2.4 Agreements shall address the secure transfer of business information between the Organization and external parties.

13.2.5 Information involved in electronic messaging shall be appropriately protected.

13.2.6 Requirements for confidentiality or non-disclosure agreements reflecting the Organization's needs for the protection of information shall be identified, regularly reviewed and documented.

14. SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

14.1 SECURITY REQUIREMENTS OF INFORMATION SYSTEMS

Security objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

14.1.1 The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.

14.1.2 Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.

14.1.3 Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

14.2 SECURITY IN DEVELOPMENT AND SUPPORT PROCESS

Security objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.

14.2.1 Procedures or rules for the development of software and systems shall be established and applied to developments within the organization.

14.2.2 Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.

14.2.3 When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

14.2.4 Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.

14.2.5 Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.

14.2.6 Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.

14.2.7 The organization shall supervise and monitor the activity of out sourced system development.

14.2.8 Testing of security functionality shall be carried out during development.

14.2.9 Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.

14.3 TEST DATA

Security objective: To ensure the protection of data used for testing.

14.3.1 Test data shall be selected carefully, and protected and controlled.

15. SUPPLIER RELATIONSHIP

15.1 INFORMATION SECURITY IN SUPPLIER RELATIONSHIPS

Security objective: To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.

15.1.1 **This requirement is mandatory to the IT Department only; other departments are recommended to follow where possible.**

Information security requirements for mitigating the risks associated with supplier's access to the Organization's assets shall be agreed with the supplier and documented.

15.1.2 All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the Organization's information.

15.1.3 **This requirement is mandatory to the IT Department only; other departments are recommended to follow where possible.**

Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.

15.2 SUPPLIER SERVICE DELIVERY MANAGEMENT

Security Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.

15.2.1 Organizations shall regularly monitor, review and audit supplier service delivery.

15.2.2 Changes to the provision of services by suppliers, including maintaining and improving existing information 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.

16. INFORMATION SECURITY INCIDENT MANAGEMENT

16.1 MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS

Security objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

16.1.1 Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.

16.1.2 Information security events shall be reported through appropriate management channels as quickly as possible.

16.1.3 Employees and contractors using the Organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.

16.1.4 Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.

16.1.5 Information security incidents shall be responded to in accordance with the documented procedures.

16.1.6 Knowledge gained from analyzing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.

16.1.7 The Organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

17. INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

17.1 INFORMATION SECURITY CONTINUITY

Security objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and

to ensure their timely resumption. Information security continuity shall be embedded in the Organization's business continuity management systems.

17.1.1 A managed process shall be developed and maintained for business continuity throughout the Organization that addresses the information security requirements needed for the Organization's business continuity.

17.1.2 Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security.

17.1.3 Plans shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.

17.1.4 A single framework of business continuity plans shall be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.

17.1.5 Business continuity plans shall be tested and updated regularly to ensure that they are up to date and effective.

17.2 REDUNDANCIES

Security Objective: To ensure availability of information processing facilities.

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

18. COMPLIANCE

18.1 COMPLIANCE WITH LEGAL AND CONTRACTUAL REQUIREMENTS

Security objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

18.1.1 All relevant statutory, regulatory and contractual requirements and the Organization's approach to meet these requirements shall be explicitly defined, documented, and kept up to date for each information system and the Organization.

18.1.2 Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.

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

18.1.4 Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.

18.1.5 Users shall be deterred from using information processing facilities for unauthorized purposes.

18.1.6 Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.

18.2 INFORMATION SECURITY REVIEWS

Security objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.

18.2.1 The Organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.

18.2.2 Managers 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.

18.2.3 Information systems shall be regularly reviewed for compliance with the Organization's information security policies and standards.

*** END ***