Section 1. Information Security Policy

Objectives

To strengthen awareness of users and stakeholders regarding information security and ensure that they have acknowledged their responsibilities and risk control practices. The organisation thus sets forth Information Security Policy and Measures as follows:

1.1.1 Management Directions for Information Security

1) Policy for Information Security

1.1) The organization is required to have a written Information Security Policy in place, the content of which must be prior approved by the President of the Board of Directors or by a c-suite executive entrusted by the President.

1.2) The organization shall disseminate the Policy for acknowledgement and compliance of users and external organisations. Such dissemination must be conducted through a platform that is easily accessible.

2) Review of the Information Security Policy

2.1) The IT Department shall assess and review the Information Security Policy as required by the provision outlined under Section 2.5 Policy Review.

Section 1.2 Organization of Information Security

Objectives

To formulate measures to monitor, supervise and track responsibilities that concern safeguarding of information system used by different departments within the organisation. Moreover, it is aimed to be a guideline for the use of mobile devices to ensure that its alignment with the Information Security Policy.

1.2.1 Internal Organization

1) Information Security Roles and Responsibilities

1.1) Divisional executives shall define responsibilities of personnel in safeguarding information security in writing, the outline of which must be aligned with the Information Security Policy.

2) Segregation of Duties (SOD)

2.1) Divisional executives shall ensure the segregation of duties to clearly disperse critical functions and responsibilities of information security to facilitate cross-checking between entities.

3) Contact with Authorities

3.1) The IT department shall prepare a contact list providing all essential contact information such as that of legal departments or related agencies, etc., for emergency purposes. In this regard, such contact list must be regularly updated.

4) Contact with Special Interest Groups

4.1) The IT Department shall prepare a directory of information security specialists and provide more communication options to facilitate users' subscription and coordination with the specialists, or acquisition of prompt advice in the case where an unprecedented incident takes place and affects information security. In this regard, such directory must be regularly updated.

5) Information Security in Project Management

5.1) The divisional executives shall have a risk control measure in place while also monitoring and assessing the overall performance of projects, whether they are organised internally or conducted by external suppliers.

1.2.2 Mobile Computing and Teleworking

1) Mobile Computing and Communication Securities

1.1) The IT Department shall have an adequate measure in place to ensure the security of mobile devices, considering risk exposures when a specific device is connected to internal server or used remotely.

1.2) All users using mobile devices for the purpose of connecting them to the internal information system shall comply with the Information Security Policy and be strictly aware of information security.

2) Teleworking

2.1) All users working remotely shall comply with the Information Security Policy in the same strict manner as when they are working onsite.

2.2) Any user who requires access to the organisation's information system for the purpose of teleworking must provide a sufficient reason and be prior approved by his/ her department and the nominated owner of such asset.

2.3) Any user who requires remote access shall obtain permission from the system administration prior to the access.

Section 1.3 Human Resources Security

Objectives

To formulate measures to monitor, supervise and track recruitment process, human resources management of current and former employees, or those who have been rotated.

1.3.1 Prior to Employment

1) Screening

1.1) The organisation shall conduct pre- employment/ pre- procurement screening and background check on all applicants and external parties that are to provide services within the organisation.

2) Employment Terms and Conditions

2.1) The HR Management Department shall advise personnel/ supplier to sign an employment contract or work agreement, or a supplier contract, in which all responsibilities related to information security are outlined. The users shall acknowledge and agree with the regulations set forth by the organisation by thoroughly reading and understanding the policies, rules and regulations contained therein.

1.3.2 During Employment

1) Management Responsibilities

1.1) Divisional executives shall supervise and guide personnel or suppliers of the organisation to comply with applicable IT policies and information security regulations enforced by the organisation.

2) Information security awareness, education and training

2.1) The IT Department shall define available channels from which personnel can acquire knowledge and understanding about the Information Security Policy, as well as their own roles and responsibilities regarding information securities prior to onboarding with the Company.

2.2) The IT Department shall regularly provide training about general operations. Such training must be led by the department responsible for each matter to ensure that employees can learn and clearly understand the topics such as workflow system, applications, basic troubleshooting techniques, legal and regulatory compliance, etc.

2.3) The IT Department shall regularly provide training about and strengthen awareness on information security to ensure that employees can learn and understand related topics and be able to perform their duties and responsibilities in a preferable and secure manner.

3) Disciplinary Process

3.1) The organisation shall apply a disciplinary punishment against users who violate or breach applicable IT policies and information security regulations, or any work procedures that concern information security.

1.3.3 Termination or Change of Employment

1) Termination or Change of Employment Responsibilities

1.1) The HR Management Department shall formulate written regulations that require personnel and external organisations to be responsible for information security subsequent to their termination or change of employment.

1.2) The HR Management Department shall encourage strict compliance of personnel and external organisations with applicable regulations.

Section 1.4 Asset Management

Objectives

To ensure that the organisation's assets and information system have been safeguarded at an adequate level in order to mitigate potential risks of unauthorised disclosure, as well as to prevent misuse and damages caused to information assets of the organisation.

1.4.1 Responsibility for assets

1) Inventory of Assets

1.1) The IT Department shall supervise and advise its department to provide an asset account for appropriate asset management and control. In this regard, such account must be updated on a regular basis.

2) Ownership of Assets

2.1) The manager of the IT Department shall require an appropriate nomination of asset owner, who is to monitor and be responsible for the respective assets.

3) Acceptable Use of Assets

3.1) The IT Department shall provide a guideline for the use of assets to optimise computer management and ensure that every access is safeguarded from possible damages. Such guideline must be communicated to personnel of the organisation for acknowledgement and further compliance.

4) Return of Assets

4.1) The HR Management Department, a respective supervisor, or manager, shall advise and ensure that the organisations' personnel or suppliers serving onsite have returned all assets such as laptop, documents, keys, employee badge, which belong to the organisation, to the specified department.

1.4.2 Classification of Information

1) Classification of Information

1.1) The Organisation shall conduct asset categorisation and classification. The classification of information must incorporate applicable laws and regulations for suitability.

1.2) Internal departments shall classify information assets utilised for Company's operations and conduct classification of such information.

1.3) Internal departments shall monitor the classification of information assets according to the operation guideline outlined in the Information Security Practices.

2) Labeling of Information

2.1) The Organisation shall regulate and ensure that all filed data have been adequately safeguarded and maintained secure, starting from the processes of printing, labelling, storing, duplicating, distributing, to destroying. Such practices shall be set forth as a regulation to be complied by personnel and stakeholders to ensure that all information assets are well monitored and safeguarded.

2.2) The IT Department and nominated entities shall attach labels, based on asset accounts, and user instructions to every computer device.

3) Handling of Assets

3.1) The IT Department shall supervise and provide work procedures regarding handling of assets to prevent information leakage and misuse of such assets.

1.4.3 Media Handling

1) Management of Removable Media

1.1) The IT Department shall provide written work procedures regarding handling of medium that store removable information, which must also be updated on a regular basis. Such procedures shall be communicated to internal users for acknowledgement and further compliance.

1.2) Handling of medium that contain removable information shall be in alignment with the classification of information.

2) Disposal of Media

2.1) The IT Department shall provide an instruction for disposal of media to prevent leakage of confidential or sensitive data.

2.2) The IT Department shall formulate control measures for disposal of media by referring to internationally recognised standards.

3) Physical Media Transfer

3.1) The IT Department shall determine work procedures or regulations to safeguard information in the case where there is a physical media transfer from a specific installation or operating area.

Section 1.5 Access Control

Objectives

To formulate guidelines for information security in order to monitor access and use of information system, and to prevent unauthorised access and access gained by unpatched software, which may cause damage to information assets of the organisation.

1.5.1 Business Requirement for Access Control

1) Access Control Policy

1.1) The organisation shall develop a written Access Control Policy. Such policy must be regularly updated and internally communicated for further compliance.

2) Access to Networks and Network Service Control

2.1) The IT Department requires that all users shall submit an access request, which must be prior approved only by their line manager.

2.2) The IT Department shall strictly limit access to authorised users. Such authorisation must be based on duties, responsibilities and necessity.

1.5.2 User Access Management

1) User Registration and De-Registration

1.1) The IT Department and the nominated owners of assets shall collaboratively determine written procedures for user registration and de-registration with regular updates and internal communications for compliance.

2) User Access Provisioning

2.1) The IT Department and the nominated owners of assets shall assign or authorise each user for the use of data or information system based on their responsibilities.

2.2) The IT Department and the nominated owners of assets shall provide a document of authorisation for the use of data or information system. Such document shall be filed as proof of operations.

2.3) The IT Department and the nominated owners of assets shall set out a procedure for user access provisioning in the case where a user needs access that goes beyond their authorisation.

3) Management of Privileged Access Right

3.1) The IT Department shall store the passwords of privileged users such as administrators (root users) of the server, or administrators of an application. Such passwords can be acquired only in necessary cases.

3.2) The IT Department shall provide written procedures for the management of privileged access right and communicate such procedures to relevant parties for their acknowledgement and further compliance.

4) Management of Secret Authentication Information of Users

4.1) The IT Department shall provide written procedures for the management of secret authentication information of users with regular updates and internal communications for acknowledgement and compliance.

5) Review of User Access Rights

5.1) The IT Department and the nominated owners of assets shall provide written procedures for the review of users' authorised access to information, IT system and applications with regular updates and internal communications for acknowledgement and compliance.

5.2) The IT Department and the nominated owners of assets shall set a clear cycle of the review over access rights to information and IT system, which must be communicated to relevant parties for their acknowledgement.

5.3) During the review of user access rights, the following matters shall be taken into consideration:

1. Defined review cycles;
2. Termination of employment;
3. Change of position and duties;
4. Request for additional access.

5.4) After completing the review process, the nominated owner of assets or administrator shall keep review records. Such records shall be categorised based on cycles of review.

6) Removal of Access Rights

6.1) The nominated owner of assets and administrator shall determine written criteria for deregistration of access rights, which must be internally communicated for acknowledgement and further compliance.

1.5.3 User Responsibilities

1) Use of Secret Authentication Information

1.1) Users shall not use a password of which the structure or characteristics are too generic; for example, a vocabulary from a dictionary, user's name or a combination thereof, or a password of alphabetical order, or personal information, or a sentence/phrase which is easy to guess.

1.2) Users shall not write down, save, keep or display their passwords in proximity to the system or any device accessible by such password.

1.3) Users shall be responsible for all actions taken if it is provable that such action was done under the username and password attributed to them, or by them using an account of other users who do not have authorised access.

1.4) Users are required to comply with other password-related regulations set forth by the organisation.

1.5.4 Application and Information Access Control

1) Information Access Restriction

1.1) The nominated owners of assets and administrator shall restrict access to data, information system and functions. In this regard, the restrictions must conform to the Access Restriction Policy.

1.2) The nominated owners of assets and administrators shall provide instructions for the use of information system, including computers, applications, e-mail messaging, wireless LAN and the Internet. Access rights must be aligned with responsibilities and require prior approval by the line manager of such user.

2) Secure Log-on Procedures

2.1) The IT Department shall provide written instructions to ensure access to the information system by referring to international standards with regular updates and internal communications for acknowledgement and compliance of all personnel.

3) Password Management System

3.1) The IT Department shall provide a management system over usernames and passwords used to access the information system in order to ensure the same standard throughout.

4) Use of Privileged Utility Programs

4.1) The IT Department shall restrict the use of privileged utility programmes and delimit the use of privileged utility programmes on the information system or key computer software in order to prevent breach or noncompliance with security measures set forth.

5) Access control to program source code

5.1) The IT Department shall determine access control to programme source code and avoid unintended changes to programme source code in order to minimise the potential for errors of information system development and workflow system of the organisation.

Section 1.6 Cryptography

Objectives

To formulate cryptographic procedures and ensure that the information system maintains the confidentiality of all information, self-authentication, and/or to adequately and efficiently prevent unintended changes by unauthorised users with guidelines as follows:

1.6.1 Cryptographic Controls

1) Policy on the Use of Cryptographic Controls

1.1) The IT Department shall formulate the use of cryptography measures, which must suit potential risks to each classification of information defined.

2) Key Management

2.1) The IT Department shall provide key management procedures that extend to the key management life cycle, as well as to consistently monitor compliance with applicable policies and such procedures.

Section 1.7 Physical and Environment Security

Objectives

To formulate prevention measures that are to be taken to monitor use and physical maintenance of information system and information devices, which are supporting infrastructures of the organisation's information system, to ensure that it is readily available for use, and to prevent unauthorised access to and disclosure of information assets.

1.7.1 Secure Area

1) Physical Security Perimeter

1.1) The organisation shall consider and secure physical security perimeter, which consists of enclosed boarding surrounding rooms, entry and exit points and adequate security system.

2) Physical Entry Controls

2.1) The organisation shall limit access to operations centres and locations in which critical cyber assets are housed, to which access is restricted to only authorised personnel.

2.2) The list of personnel authorised to access operations centres and locations in which critical cyber assets are housed must be consistently examined, improved and updated.

2.3) The IT Department shall limit physical access to secure areas including computer rooms and system administrator areas to authorised personnel only. All access to computer rooms must be logged with details of such person, time of access, purposes of access, and such log must be regularly examined.

3) Securing Offices, Rooms, and Facilities

3.1) The IT Department shall configure and install a physical security system to safeguard operations centres, locations in which critical cyber assets are housed, computer rooms, system administrator areas, and information devices used for the operations, from damage and unauthorised access.

4) Protecting Against External and Environmental Threats

4.1) The IT Department shall monitor and supervise to ensure physical security protection has been configured and installed to prevent external threats, including both human-caused and natural disasters such as fire, floods, earthquake, explosion, civil disorder, epidemic etc.

5) Working in Secure Areas

5.1) The IT Department shall have guidelines for physical security for those who work in secure areas, including operational areas and data center rooms, and shall require rigorous compliance with such guidelines.

6) Delivery and Loading Areas

6.1) The IT Department shall ensure that unauthorised persons are not able to access restricted areas. Delivery/ loading areas and preparation or assembling points of information devices to be used in computer rooms must be clearly designated, organised and marked to avoid unauthorised access.

1.7.2. Equipment

1) Equipment Setting and Protection

1.1) The IT Department shall locate information devices within a secure room or location. Safety cabinets that house routers and networking hardware must invariably be locked and shall be unlocked only by authorised technicians for maintenance or reconfiguration in order to reduce risks of unauthorised access.

2) Supporting Utilities

2.1) The IT Department shall ensure system failure prevention equipment and supporting utilities are installed within computer rooms including fire protection equipment, smoke detectors, uninterruptible power supply (UPS), temperature/humidity controllers, water leak detectors, error monitoring system, etc. In this regard, all equipment must be well maintained and readily available.

3) Cabling Security

3.1) The IT Department shall ensure that installation and maintenance of communication cables within operations centres and computer rooms are in line with the applicable industrial security standards in order to prevent unauthorised access, data interception, or physical damage.

4) Equipment Maintenance

4.1) The IT Department shall ensure there are maintenance services provided for all major processing information devices used at the operational level and supporting utilities in a timely manner and in accordance with the requirements of respective manufacturers in order to facilitate their consistent operations and availability.

4.2) The IT Department shall ensure maintenance activities are logged. Moreover, detected issues and deficiencies of devices must be recorded for further assessment and improvement to achieve invariable availability.

5) Removal of Assets

5.1) The person responsible for monitoring areas and premises that require security safeguard shall not allow relocation of information assets to outside of the organisation, except for the case where such removal is permitted by an entrusted approver.

5.2) Users shall not take information devices, assets or software out of the organisation, except for the case where such removal is permitted by an entrusted approver.

5.3) The IT Department shall have written procedures for removal of assets in place and ensure they are regularly updated and communicated to internal users for acknowledgement and further compliance.

6) Security of Equipment and Asset Off-Premises

6.1) It prescribes that executives of at least the divisional level shall have authority to allow use of information devices off-premises. Such devices used off-premises must be protected to prevent potential damage and possible risk exposures must be taken into consideration.

6.2) The IT Department shall formulate security measures to safeguard information assets utilised off-premises in order to minimise risks caused by the use of such devices or assets outside the organisation.

7) Secure Disposal or Re-Use of Equipment

7.1) Users shall recheck such devices in which there is a storage unit to reassure that critical cyber data or licensed software have already been adequately removed, transferred or destroyed based on the classification of data prior to the disposal or reuse of such devices.

7.2) The IT Department shall have procedures in place for the destroying of data or information assets, and measures or techniques for further disposal of data and reuse of information devices. In this regard, such procedures must correspond to the classification of data.

7.3) The IT Department shall assign a person to be responsible for disposal of information assets stored in storage media, which are no longer necessary for the operations of the organisations.

8) Unattended User Equipment

8.1) The IT Department shall formulate protection measures to safeguard computers and information devices which are left unattended in order to prevent unauthorised access.

8.2) Administrators shall require users to not allow other persons to access their computer hardware or the information system and to fill in correct username and password prior to access to such computer.

8.3) Users shall immediately log off from the information system, active computer system and computer hardware once they no longer use it or after completing an operation.

8.4) Users shall lock their computer screen or that of critical devices when it is not in use or when they are not in the proximity to such hardware.

9) Clear Desk and Clear Screen Policy

9.1) Administrators shall ensure that all users have locked their screens when the system is not currently used ; for example, Session Time Out and lock screen, etc.

9.2) Users shall not leave critical information assets such as physical documents or storage media unattended in a non-secure 1. area, public space, or location in which such assets are easily found. Users shall house information assets in proper locations as well as having prevention measures in place to restrict unauthorised access.

9.3) Users shall not store critical data in their desktop folder. They are required to create secure folders on the computer and adequately limit usage to prevent unauthorised access.

Section 1.8 Operations Security

Objectives

To set out control measures to ensure there are explicit guidelines and secure procedures for information security operations and communications.

1.8.1 Operations Procedures and Responsibilities

1) Documented Operating Procedures

1.1) The IT Department shall provide information operations procedures in writing. Personnel responsibilities must be defined based on clear business structures to ensure they are able to discharge their duties correctly and in compliance with the Information Security Policy enforced by the organisation.

1.2) Sections in the IT Department shall provide handbooks, system manuals and knowledge database to ensure that relevant parties deliberately understand all workflows, nature of work and process.

1.3) Sections in the IT Department shall invariably review such practices, handbooks, system manuals and knowledge database to ensure that they are readily available, accessible, and are communicated to all stakeholders for acknowledgement and further compliance.

2) Change Management

2.1) The IT Department shall monitor the implementation of structural change management, workflows and the information system in order to place transformation, correction, or any activity that affects the work system under control. In this regard, the provisions contained herein under **Part 5.1 Change Management Policy** shall be complied.

3) Capacity Management

3.1) Administrators shall monitor performance of work systems and major information devices to ensure their continuity and efficiency.

3.2) Administrators shall evaluate capacity and sufficiency of information assets such as use of servers and network devices such as CPUs, memory units, disks, bandwidth, etc.; and shall conduct resource planning to ensure the information system is adequately efficient and capable of accommodating future use.

4) Separation of Development, Testing and Operational Environments

4.1) The IT Department shall monitor and direct separation of system development, testing and operational environments.

4.2) The IT Department shall ensure authorisation of access to each specific environment and assigning custodianship is clearly performed. Operational results must be reported to the line manager. In the case where a problem is detected, such problem and its solutions must be logged and further reported to the line manager for his/her acknowledgement.

1.8.2 Protection from Malware

1) Controls Against Malware

1.1) The IT Department shall formulate measures to detect, prevent and restore system to safeguard assets from malware. Moreover, awareness of all stakeholders should be adequately reinforced.

1.8.3 Back up

1) Information Backup

1.1) The IT Department shall outline measures concerning information backup and consistent backup cycles for critical information to prevent losses of data.

1.2) Nominated owners of assets shall make extra copies of data, or require consistent backup of information, and conduct backup data testing to ensure that data will readily be restored for further use.

1.3) Users shall be responsible for backing up data to an external storage such as external hard disks on a regular basis. Such data must be stored in proper media which are not exposed to risks of data leakage.

1.8.4 Logging and Monitoring

1) Event Logging

1.1) Administrators shall sufficiently log events concerning information security for further assessment.

1.2) Administrators shall monitor the use of information system. Results of such monitoring shall be reviewed on a consistent basis to identify abnormal activities.

1.3) Administrators shall monitor and direct logging of fault events that involve information use, including analysis, correction and provision of prevention approaches to prevent potential recurrence of such problems.

2) Protection of Logged Information

2.1) Administrators shall ensure protection of information, event and evidence logging system available on the information system against modification, destruction and unauthorised access.

3) Administrator and Operator Logs

3.1) Administrators shall require logging of activities by administrators and operators who are involved in system operations; for example, time of system activation and deactivation, modification of system settings, system errors and actions taken for correction. In this regard, such activity logs must be regularly reviewed.

4) Clock Synchronisation

4.1) Administrators shall ensure and direct clock synchronisation for all information devices and system throughout the organisation based on the legal and universal time.

4.2) Administrators shall examine the clock of information devices and system of the organisation, as well as updating it on a regular basis in order to prevent incorrect timestamps.

1.8.5 Control of Operational Software

1) Installation of Software on Operational Systems

1.1) The IT Department shall provide work procedures and measures to guide the installation of software on the operational systems in order to limit and prevent installation of unauthorised software carried out by users.

1.2) The IT Department shall define a list of standard software allowed to be installed on the organisation's computer devices in writing with regular updates. Such list must be communicated to internal users for acknowledgement and compliance.

1.8.6 Technical Vulnerability Management in Hardware and Software

1) Management of Technical Vulnerabilities

1.1) The IT Department shall identify potential technical vulnerabilities of the organisation's information system at least on a yearly basis.

1.2) Administrators shall preserve and maintain the state of being secure of the information system on a regular basis, including identifying technical vulnerabilities, assessment of risk exposures derived from detected vulnerabilities and improvement of such vulnerabilities.

2) Restrictions on Software Installation

2.1) Users shall comply with the regulations on restrictions of software installation and shall not install any pirated software on the organisation's computers.

1.8.7 Information Systems Audit Considerations

1) Information System Audit Controls

1.1) The IT Department shall provide information system audit plans that are aligned with the risks having been assessed through, for example, vulnerability assessment.

1.2) The IT Department shall inform relating entities in advance every time before they audit the information system.

1.3) The IT Department shall define the scope of technical audit tests to ensure that it covers critical vulnerabilities and shall control such audit tests to not affect normal operations. In the case where any technical audit test may affect system availability, such test must be conducted outside business hours.

Section 1.9 Cybersecurity Communications

Objectives

To formulate control measures for network management and transmission of information via computer networks, either internally or externally, for the purpose of cybersecurity.

1.9.1 Network Security Management

1) Network Controls

1.1) Administrators shall control and monitor network security management to prevent threats and safeguard information system and applications operating on the computer network, including information exchanged thereon.

2) Security of Network Services

2.1) Administrations shall ensure that security characteristics, service levels and network management needs are defined in network services agreements or contracts, both for services provided internally or by external suppliers.

3) Segregation in Network

3.1) The IT Department shall ensure segregation in network as deemed appropriate by taking the access demands of users, impacts against information security, and priority of data available on such network into consideration.

1.9.2 Information Transfer

1) Information Transfer Policies and Procedures

1.1) The IT Department shall monitor and ensure to have information transfer procedures in place, which are suitable for specific types of communications, types of information and classification of data.

2) Agreements on Information Transfer

2.1) The IT Department shall monitor and ensure to settle written agreements on information transfer, whether internally or between organisations.

2.2) In transferring information between organisations, such transfer must be prior approved by the nominated owner of the asset every time and conducted under a written agreement. Moreover, the transfer shall be subjected to specific terms and conditions and be protected based on data classification.

3) Electronic Messaging

3.1) The IT Department shall have a measure in place to monitor electronic messaging such as e-mail, EDI (Electronic Data Interchange), instant messaging, etc. Critical email messages need to be adequately protected from accessing, editing, interrupting attempts by unauthorised users.

4) Confidentiality or Non-Disclosure Agreements

4.1) Divisional executives must procure their personnel and external suppliers working for the organisation to sign a written confidentiality or non-disclosure agreement.