HPOL#03
Personnel Security Infrastructure

(Version 1.0)

Table of Contents

3.1. SCOPE AND OBJECTIVES

Information is the lifeblood of every organization and, regardless of its source, is a valuable asset. Information Security is therefore an organizational risk management issue. It is necessary to ensure that government organization information, which is generally accessible (in hard or soft copy), is protected from inappropriate access, disclosure or modification. Protection of information assets must be commensurate with defined value and risk.

Personnel at all levels are required to contribute to maintaining a high level of information security. Security is an objective where staff members are to be active agents and is an integral part of everybody's job profile and objectives.

A primary component of a security system is awareness of the components of the security systems and responsibilities for security. Each user has a duty to act responsibly and within security guidelines when utilizing assets and computing services. The security policies articulate direction and decisions concerning security, however, all users must be aware of the security features and policies relevant to them and why they are in place.

Security considerations will be addressed through the hiring process and in staff accountabilities and responsibilities to support the security posture. This policy applies to new employees, re-hired employees, transferred, or promoted employees, as well as third parties such as temporary staff, contractors, and consultants.

3.2. POLICY STATEMENT

3.2.1. SECURITY IN JOB DEFINITIONS

2.1.1. Including Security in Job Responsibilities

3.2.1.1.1. All job roles and responsibilities must be documented.

Explanatory Notes

Job roles and responsibilities must include general as well as specific responsibilities for implementing or maintaining security.

3.2.1.1.2. All personnel must be provided with awareness programmes to communicate to them their job roles and responsibilities.

2.1.2. Personnel Screening

3.2.1.2.1. Background checks will be performed on all personnel performing sensitive or critical job roles before they are selected for a position or transferred to a position.

Explanatory Notes

Background checks on personnel will include but not be limited to government organization employees, temporary personnel, contract personnel and third party service providers.

3.2.1.2.2. Periodic background checks are required on all personnel who work in sensitive or critical job roles.

3.2.1.2.3. Information provided by personnel, at the time of recruiting must be subjected to verification procedures.

3.2.1.2.4. All supervisory roles are responsible for the performance and conduct of the staff personnel reporting to them.

Explanatory Notes

Managers / supervisors are required to monitor performance and conduct of each of their staff, as well as

to assess the impact on the security of information resources to which the staff has access.

2.1.3. Non Disclosure Agreements

3.2.1.3.1. All users of Information Assets will be required to accept non-disclosure obligations by signing non-disclosure agreements.

Explanatory Notes

Users are required not to disclose information derived as a result of their access to information systems of government organizations to unauthorized parties.

3.2.1.3.2. All users will be required to periodically re-affirm their non-disclosure obligations by signing non-disclosure agreements.

2.1.4. Terms and Conditions of Employment

3.2.1.4.1. All personnel must sign terms and conditions of employment as an indication of acceptance.

Explanatory Notes

The terms and conditions of employment must contain reference to:

- *The employee's legal and information security related responsibilities;*
- *The extent and duration of the responsibilities; and*
- *An indication of management action in case the terms of employment are violated.*

2.1.5. Performance Evaluation

3.2.1.5.1. Security responsibilities will be included in the performance evaluation of personnel assigned significant security roles.

Explanatory Notes

Personnel assigned significant security roles would include security administrators, network administrators, etc.

3.2.2. USER TRAINING

2.2.1. Information Security Awareness and Training

3.2.2.1.1. Personnel must be given training programmes with regard to information security and security awareness.

Explanatory Notes

Those who are involved with technical security responsibilities are required to learn additional security skills that correspond to their specific job role.

3.2.2.1.2. Details of training and certificates (if any) issued during the training must be documented and maintained in each personnel profile.

3.2.2.1.3. The government organization provides appropriate new user training and ongoing awareness training.

Explanatory Notes

New user training and ongoing awareness training is provided in order to ensure that staff is well versed on security requirements and properly equipped to support the security posture of the organization.

3.2.2.1.4. The government organization ensures that formal and informal security reminders are delivered to staff.

3.2.2.1.5. The government organization allocates sufficient time for new employees to review the security policies, standards, and procedures and will allocate sufficient time, on an annual basis, for existing employees to review requirements.

3.2.3. USER RESPONSIBILITIES

2.3.1. Privacy of Information

3.2.3.1.1. All employees, consultants, or contractors with access to personal or confidential information are required to respect the confidentiality and security of that information.

2.3.2. Protection of Intellectual Property

3.2.3.2.1. All results of the endeavours of employees, consultants, or contractors under the direction of the government organization are classified as government organization intellectual property and are owned by the government organization.

Explanatory Notes

All such individuals must support the security of Intellectual property. Intellectual property is defined as any trademarks, patents, copyrights, inventions, proprietary organization information, and other collections of information deemed to be important to the functions of the government organization.

2.3.3. Regulatory Requirements

3.2.3.3.1. Training programmes will be held for government organization employees, consultants, or contractors on applicable regulations.

Explanatory Notes

The functions of government organizations are subject to many regulatory issues. The protection of citizen and other information is required to protect the interests of the government organization and its clients. The objective of the training programmes is to ensure that the participants understand and adhere to applicable regulations.

2.3.4. User Awareness

3.2.3.4.1. Government organization employees, consultants, and contractors will ensure that they participate and support the user awareness requirements of the organization.

2.3.5. Personal Use of Systems

3.2.3.5.1. Government organization employees, consultants, and contractors will refrain from using organization resources for personal or private business purposes or for entertainment.

Explanatory Notes

The resources of the government organization are intended to support the functions of the organization. Use of these resources for personal activities can decrease the effective utilization of those resources and increase the cost to the government organization.

2.3.6. Appropriate Use of E-mail

3.2.3.6.1. The use of E-mail shall be governed by the "Internet and Electronic Mail Security" Policy.

Explanatory Notes

Electronic mail provides an expedient method of creating and distributing messages both within the government organization and outside of the organization. The user of the government organization E-mail system is a visible representative of the organization and must use the system in a legal, professional and responsible manner to uphold the reputation of the organization. The E-mail system has been put in place to support organization correspondence and should be utilized as such.

2.3.7. Appropriate Use of Information Systems

3.2.3.7.1. The information systems of the government organization must not be used in such a way that is or is perceived to be illegal, unethical or with a specific intention to deceive or contribute harm to the organization.

Explanatory Notes

The use of information technology processing systems is an integral part of the functions of the government organization. The users of all organization information systems are required to utilize the systems in a legal and responsible manner. The government organization has implemented security measures to protect the information and systems. The users have a responsibility to adhere to and apply the measures appropriately.

2.3.8. Appropriate Use of the Internet

3.2.3.8.1. The use of Internet shall be governed by the "Internet and Electronic Mail Security" Policy.

Explanatory Notes

The Internet can be used as a source of information and provides cost effective communication. Without adequate security controls, it can also be a source for security exposure. All employees or users who access the Internet through services supplied or contracted by the government organization are considered to be representatives of the organization. All users of the Internet on behalf of the government organization are required to utilize that access in a legal and responsible manner. Use of the Internet is expected to be for organization purposes.

2.3.9. Appropriate Use of Software

3.2.3.9.1. Government organization employees, consultants, and contractors will not install software on organization assets that is not approved by the organization.

Explanatory Notes

Limitations and restrictions on the use of software are included in the software licensing agreements that accompany each software package.

2.3.10. Protection of Portable Equipment

3.2.3.10.1. Government organization employees, consultants, and contractors will protect all portable assets, including information, to a degree similar to that provided within the organization offices.

Explanatory Notes

Portable computing equipment is a very valuable asset of the government organization for both the value of the equipment as well as the value of any information contained therein. The use of portable computing equipment can expose the government organization to disclosure of sensitive information or loss of a valuable

asset. Due care and attention is required to protect the portable computing assets and the contained information.

2.3.11. Virus Protection

3.2.3.11.1. Virus protection shall be governed by the "Virus and Malicious Software Protection" Policy.

Explanatory Notes

A virus is any software that can negatively impact or cause harm to a system, data or networks. There are several forms of virus and methods by which they can cause harm. Viruses that are introduced into any system are, at best, a nuisance requiring time and effort to deal with them and, at worst, have the ability to seriously damage or destroy data or systems that will require extensive reconstruction and recovery. Government organization employees, consultants, and contractors will be vigilant in awareness that externally sourced media or externally received information may contain virus software and will take reasonable measures to protect the organization from this threat.

2.3.12. Security of Electronic Office Systems

3.2.3.12.1. Vulnerabilities of information in office systems are controlled to minimize the risk of accidental disclosure.

Explanatory Notes

Examples of information in office systems includes but is not limited to the confidentiality of telephone calls, storage of faxes, and the handling of mail.

3.2.3.12.2. Categories of staff, contractors and business partners authorized to use government organization systems, and the locations from which the systems may be accessed, is defined and managed by the organization employee to whom those individuals report.

2.3.13. Public Systems

3.2.3.13.1. There is a formal authorization granted by the information owner before government organization information is made publicly available.

Explanatory Notes

The integrity of the information is protected by the publisher to prevent unauthorized modification, in accordance with data protection legislation.

3.2.4. RESPONDING TO SECURITY INCIDENTS AND MALFUNCTIONS

2.4.1. Reporting Security Incidents, Weaknesses and Malfunctions

3.2.4.1.1. Defined channels for the reporting of security incidents are defined for employees.

Explanatory Notes

Reporting channels may include immediate supervisor or manager and should include the Chief Innovation Officer (CIO).

3.2.4.1.2. Security violations and problems are immediately reported to designated personnel.

Explanatory Notes

The reporting of security violations ensures that the escalation process can be invoked to take corrective action.

3.2.4.1.3. Individuals are granted anonymity in the event they are reporting a breach caused by another employee.

3.2.4.1.4. Any form of retaliation, except as defined by formal disciplinary actions for willful, or for repeated accidental or inadvertent breaches, against an individual reporting a breach or violation is prohibited and cause for disciplinary action.

3.2.4.1.5. The identifying party does not disclose to non-government organization employees, or to unaffected organization employees, breaches in security policy or the loss or inappropriate disclosure of information.

Explanatory Notes

The government organization Communications function performs the internal and public disclosures, as required.

3.2.4.1.6. Where legally required, the government organization discloses violations to the appropriate authorities.

Explanatory Notes

Where a legal requirement does not exist, the government organization assesses disclosure requirements on a case-by-case basis.

2.4.2. Learning from Incidents

3.2.4.2.1. The government organization requires that processes be developed to analyze security incidents and identify proactive measures to be undertaken to avoid similar incidents in future.

2.4.3. Disciplinary Process

3.2.4.3.1. The government organization must develop a formal procedure for disciplinary actions for violation of organization Information Security Policies, and the organization will take legal action against any user found to be violating the law, as per the defined procedure.

3.2.5. EXIT OF PERSONNEL

2.5.1. Terminations and Separations

3.2.5.1.1. All individuals to be terminated or separated from the government organization should maintain the confidentiality of sensitive organization information that they had access to during their employment.

3.2.5.1.2. Upon termination, separation or expiration of contract, all employees, contractors, consultants, and temporary staff must return all organization assets and all copies of organization information received or created during the performance of the contract.

3.2.5.1.3. Appropriate notifications and actions are made to ensure that logical and physical access is terminated, and to ensure that all organization property is returned.

Explanatory Notes

This will include at a minimum, notification to network and application administrators, physical site managers, human resources, and management.

3.2.5.1.4. All involuntarily terminated staff are escorted and monitored through the premises as they gather their personal effects.

3.2.5.1.5. Notification is disseminated to all staff upon termination or separation of individuals.

Explanatory Notes

This is to ensure that staff do not inadvertently provide unauthorized access to terminated or separated individuals.

2.5.2. Exit Interviews

3.2.5.2.1. All employees must be interviewed before their departure from the government organization, and details of the interview should be documented for future reference.

Explanatory Notes

The aspects covered in the interview would include but not be limited to the reason/s for leaving, problems faced during employment, encounter of information security related incidents, and suggestions for improvement of the organization.