Information Security Policy Statement, v 1.0

Information Security Policy Statement, v 1.0

General

- With the networking of government organizations and the establishment of databases with personal records pertaining to citizens, the Department of Pensions (DP) will need to balance between giving employees and citizens, real-time access to applications and information, and addressing the corresponding concern for the security of information and information systems.

- Information is a valuable asset. It is necessary to ensure that the information of the Department of Pensions is accurate, timely, relevant and appropriately protected from unauthorized access, disclosure, modification, disruption or deletion.

- Therefore it is necessary to ensure that handling, access, use, processing and disclosure of information is consistent with the information security policy.

- Ensuring the implementation of the policy and the security of information and information systems is not only a technical issue, but also involves DP's processes, structures, personnel, physical security, operational procedure, roles and responsibilities, reporting mechanisms, and accountability.

- The Government organization must ensure the confidentiality, integrity and availability of information and services, ensure business continuity and minimize risk. This will preserve the confidence of the public, minimize financial loss and ensure the productivity of the organization.

Policy

1.0 Organizational security

1.1 There should be clear leadership for identifying information security goals, setting priorities, approving plans, for providing resources and for investments, for monitoring, and for the introduction, implementation and awareness of information security. An organization-wide understanding of the roles and responsibilities, threats and risks should be created to take adequate security measures, establish security organization and instill the security culture.

1.2 Independent information security reviews must be performed to identify practices and infrastructure that are not consistent with the information security policies, procedures and standards which could expose government organization to risk.

2.0 Asset classification

2.1 A risk assessment process should be established that addresses the sensitivity and the criticality of information, so that attention is given to information assets proportionate to their sensitivity.

2.2 Information assets will be assigned classifications based on their susceptibility to risk. Criteria for asset classification should include but not be limited to confidentiality, integrity and availability. Protection of information assets must be commensurate with defined value and risk. Different sensitivity classifications must entail separate handling requirements.

2.3 The Government organization assets must be listed in an information asset inventory.

2.4 Information ownership must be clearly assigned. Each information asset must have a nominated owner and custodian. Authority to originate, modify, and delete specific types of information should be defined. Methods of protecting the assets and implementing the controls to protect them should be defined.

3.0 Personnel security

3.1 All job roles and responsibilities, including security roles and responsibilities must be defined and documented. 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. All users of information assets will be required to sign non-disclosure agreements (NDAs).

3.2 All persons to be terminated from the Government organization should maintain the confidentiality of sensitive organization information that they had access to during their employment. Responsibilities for performing employment termination or change of employment should be clearly defined and assigned. Penalties must be imposed on persons violating the NDAs indicated in 3.1.

3.3 Upon termination or expiration of contract, all employees, contractors, consultants, and temporary staff must return all the Government organization's assets and all copies of organization information received or created during the performance of the contract. Appropriate notifications and actions are made to ensure that logical and physical access is terminated, and to ensure that all organization property is returned.

4.0 Privacy issues for outside entities

4.1 Access to restricted / confidential / internal information or data of the organization must be provided to third-parties only if they have a legitimate business need for the same and must be controlled to avoid intentional / unintentional disclosure. Non-disclosure agreements to be signed where appropriate and necessary.

4.2 Risks to the organization's information and information systems, from processes involving external parties should be identified and appropriate controls implemented before access is granted.

5.0 Physical security

5.1 The physical security perimeters will be clearly defined based on risk assessments for the area and its contents.

5.1.1 The areas to be considered and assessed for risk, treated and protected by appropriate entry controls are,

- Established areas (offices, rooms, facilities)
- Equipment positioning
- Environmental controls
- Power supply
- Disposal of media

6.0 Acquisition and maintenance

6.1 When systems are purchased, the Government organization should ensure that software not necessary for the mandate and functions of the organization are not included in the system.

6.2 All statements of business requirements for new information systems or enhancements to existing information systems must specify control and system security requirements. *[Section 7.2.1, HPOL#07-v1.0-Acquisition, Development and Maintenance of Software]*

6.3 Before connecting new acquisitions to an information system, a formal testing process should be followed and it should be ensured that the new acquisition functions properly and will not adversely impact the existing information system.

7.0 Communications and operations

7.1 Operating procedures to implement all components and requirements of the Government organization's information security policies, procedures, standards, and guidelines, shall be documented, maintained and updated, and made available to users who need them.

7.2 All changes to information systems environment must be documented, reviewed, authorized, and tested (using a test environment) prior to being made operational.

7.3 The Government organization must minimize risk due to system failures and to safeguard the integrity of information processing facilities and software.

7.4 All application and operating systems software, data (including databases), applications, operating systems, user configuration information and hardware configuration information (where applicable) must be backed up.

7.5 Back up copies of information and software should be taken and tested regularly in accordance with the agreed backup policy

7.6 Historical records in the form of logs, call records, registers, etc must be maintained for audit purposes

8.0 Logical access control

8.1 Formal procedures must be in place to control the allocation of access rights to information systems and services, and to prevent unauthorized access. Access to information must be specifically authorized in accordance with the Government organization's access control policy and procedures.

8.2 The Government organizxation must draft its User Registration and Termination Procedures, and registration and termination of users must be in accordance with these procedures. All users of information resources must have a unique user ID and authorization from the system owner or management, to access the government organization's information assets.

8.3 Allocation of privileges should be restricted and controlled. All privileges must be allocated through a formal authorization procedure as and when required on a "need to know" basis as determined by the system owner. Detailed records must be maintained for all privileges allocated.

8.4 All external connections by business partners and citizens must be documented and authorized in accordance with the defined "request for connectivity" procedure.

9.0 Business continuity

9.1 The Government organization must develop, implement and maintain business continuity plans and strategies. Business continuity considerations will be conducted in light of all organizational processes.

9.2 The Government organization must develop and maintain a business continuity strategy based upon risk assessments.

10.0 Compliance measurement

10.1 The design, operation, management and use of information systems and related facilities must comply with all applicable legal, regulatory and contractual security requirements.

11.0 Information systems acceptable use

11.1 Users should use information resources for business purposes for which they have been authorized.

11.2 Introduction of unauthorized copies of licensed software and hardware (piracy / copyright and/or patent infringement) to information resources and the copying of such material is prohibited.

11.3 The storage, processing, or transmittal of such unauthorized copies of licensed software and hardware by employees, contractors, or associates, is strictly prohibited.

11.4 Introduction of freeware and shareware software whether downloaded from the Internet or obtained through any other media to the Government organization's information systems will be subject to a formal evaluation and approval process.

11.5 The introduction, storage, processing, or transmittal of pornographic material or material that is obscene, misleading or offensive to any ethnic group, gender, accepted religion, culture or to any accepted tradition of Sri Lanka, on the Government organization's information systems, by government organization employees, contractors, or associates, is strictly prohibited.

12.0 Internet and email

12.1 The Government organization must minimize risks associated with Internet and e-mail services, and define controls against the threats of unauthorized access, theft of information, theft of services, and malicious disruption of services.

12.2 The following must never be sent over the Internet unless it has first been encrypted: DP's sensitive and confidential information, source code unless specifically known to be in the public domain, parameters that can be used to gain access to goods or services.

12.3 Users must ensure that postings on to mailing lists, public news groups and related websites do not reveal details of the Government organization's internal functioning, infrastructure or potential vulnerabilities in the organization's information security infrastructure.

12.4 Each person who has log-in access to the Internet connection must have a unique user ID and password.

13.0 Malware

13.1 Virus and Malware detection infrastructure must be implemented at points where Viruses and Malware can be introduced into the Government organization's network. [Section 14.2.2.1 HPOL#14-v1.0-Virus and malicious software protection]

13.2 The government organization must implement a process to update the Virus and Malware detection infrastructure with the latest product and Virus signature updates as soon as these updates are released. [Section 14.2.1.1 HPOL#14-V1.0-virus and malicious software protection]

13.3 The installation of Virus and Malware protection software on any new potential point of entry of Viruses or Malware, or to determine that the new (potential) point of entry is covered by an existing installation of such software must be in accordance with the government organization's defined procedures. [Section 14.2.1.1 HPOL#14-v1.0-virus and malicious software protection]

13.4 The steps/decisions to be taken to protect the government organization's information system infrastructure from a new Virus or Malware, before the government organization's Virus and Malware protection infrastructure is updated to address risks, must be in accordance with the virus and Malware Contingency Plan, to be available electronically through a common staff directory, and with the Information Security Officer. [Section 14.2.1.1 HPOL#14-v1.0-Virus and malicious software protection]

14.0 Fraud

14.1 The government organization must develop a fraud management strategy defining the government organization's plan to address fraud related issues and successful deployment of fraud management controls. *[Section 16.2.1.2, HPOL#16-v1.0-Fraud Management]*

14.2 A process must be developed and implemented to identify fraud sensitive areas and assess the likelihood and impact of various types of frauds. Risk identification, Measurement and Prioritization must be performed. *[Section 16.2.1.1, HPOL#16-v1.0-Fraud Management]*

14.3 As per the Government Fraud Response Plan, prompt and effective action must be taken to minimize the risk of any subsequent losses following a fraud incident. *[Section 16.2.1.6, HPOL#16-v1.0-Fraud Management]*

15.0 Information Security Incident Management:

15.1.1 The Government organization must set up a procedure whereby all information security incidents and suspected information security incidents are reported as quickly as possible without any delay, through the appropriate management channels, to the helpdesk and to the designated information security officer in the organization, as defined in the roles and responsibilities of the organizational Information Security policy and procedures manual. *[Section 17.1.1, HPOL#17-v1.0- Information Security Incident Management]*

15.1.2 Senior management and the designated officer should respond speedily to all information security incidents, and coordinate with relevant staff in handling the incident reporting to relevant agencies. *[Section 17.1.3, HPOL#17-v1.0- Information Security Incident Management]*

15.1.3 Roles, responsibilities and procedures should be established to ensure quick and effective response to information security incidents and all employees should be alerted to possible threats and specific safeguards to be put in place. *[Section 17.1.3, HPOL#17-v1.0- Information Security Incident Management]*

- The Information and Communication Technology Agency of Sri Lanka (ICTA) is responsible for the formulation, maintenance and updating of this policy.

- Incidents to be reported by government organizations to SLCERT.