HPOL#01
Organizational Security

(Version 1.0)

Table of Contents

1.1. SCOPE AND OBJECTIVES

For government organizations to achieve its desired security posture, and to ensure that it is consistent throughout the organization, a comprehensive set of policies, which represents management's security direction, is required. As the needs of the organization and the direction of technology changes, these must be reflected in the policies to ensure that the controls remain effective.

This policy applies to all users of information assets including employees, employees of temporary employment agencies, vendors, business partners, and contractor personnel and functional units regardless of geographic location.

This Policy covers all Information Systems (IS) environments operated or contracted with third parties. The term "IS environment" defines the total environment and includes, but is not limited to, all documentation, physical and logical controls, personnel, hardware (e.g. mainframe, distributed, desktop, network devices, wireless devices), software, and information.

Constantly evolving technology entails new threats and, consequently, an increase in the risks associated with automation. An enterprise-wide understanding of the responsibilities, threats and risks should be created to take adequate security measures, establish security organization and instill the security culture.

1.2. POLICY STATEMENT

1.2.1. STANDARDS

1.2.1.1. Leadership

1.2.1.1.1. There should be clear leadership for infrastructure and technology services to set priorities, approve plans, agree investments and monitor progress, as well as to lead the introduction and awareness of new ICT infrastructure technology with specific emphasis on information security.

1.2.1.2. Additions and Changes

1.2.1.2.1. Alterations to the established security policies are made as necessary. Approval is required before altered or newly created policies may take effect.

1.2.1.2.2. Approved changes or additions to the security policy are communicated to all relevant staff.

1.2.1.3. Independent Review of Information Security

1.2.1.3.1. The implementation of Information Security policies, procedures and technical standards is to be reviewed on a periodic basis.

Explanatory Notes

The security policies and standards are reviewed to ensure they are consistent with and properly address:

- *External technology environment – opportunities and threats created by changes, trends, and new developments*
- *Internal technology environment - strengths and weaknesses resulting from the use of technology*
- *Business needs and business environment – controls remain effective from both a cost and process perspective and support the business without causing unreasonable interference*
- *Regulatory and contractual requirements*

1.2.1.3.2. This review must be carried out by experienced persons, suitably qualified for this purpose.

Explanatory Notes

An independent review of Information Security will have the following objectives: -

- *To critically review the Information Security policies, procedures and standards with a view to suggesting improvements or leading practices.*
- *To identify practices that are not consistent with the Information Security policies, procedures and standards that could expose the government organization to risk.*

1.2.1.4. Dissemination

1.2.1.4.1. The security policy is communicated and is accessible to all appropriate staff.

Explanatory Notes

Disclosure of the security policy and standards outside of the government organization is made only as needed, for example for regulatory or contractual requirements, with approval. This approval is given with the consideration that the disclosure of the policies and standards will not diminish its security posture (e.g., access controls standards may reveal possible security weaknesses).

1.2.1.5. Training and Awareness

1.2.1.5.1. It is the responsibility of the government organizations to provide general security training and awareness for all new hires and, as needed, to all current employees.

1.2.1.6. Cooperation between Organizations

1.2.1.6.1. The government organization recognizes that the maintenance of the desired level of information security may require the cooperation, support and assistance of external parties.

Explanatory Notes

The organizations must develop and maintain formal contacts with law enforcement authorities, regulatory bodies, vendors, security groups and industry forums and other service providers.

1.2.1.6.2. The extent of cooperation and transfer of information must be formalized to the extent possible.

Explanatory Notes

Such cooperation should be in the interest of the government organization and should not result in violation of the Information Security Policies of the organization, including the transfer of confidential / classified information to unauthorized third parties.

1.2.1.7. Compliance Measurement

1.2.1.7.1. Compliance with government organizational security policy is mandatory.

Explanatory Notes

All staff must comply with both the letter and spirit of all security policies.

1.2.1.7.2. Continuous compliance monitoring within government organizations must be ensured.

Explanatory Notes

Compliance with the Organizational Security Policy will be a matter for periodic review. Compliance measurement should also include periodic review for Security Quality Assurance.

1.2.1.7.3. Violations of the policies will result in corrective action by management.

Explanatory Notes

Disciplinary action will be consistent with the severity of the incident.

1.2.1.8. Waiver Criteria

1.2.1.8.1. Requested waivers must be formally submitted.

Explanatory Notes

Justification and benefits attributed to the waiver shall be specified, and approval must be obtained. The waiver should only be used in exceptional situations when communicating non-compliance with the policy for a specific period of time.

1.2.1.8.2. At the completion of the time period, the need for the waiver should be reassessed and re-approved, if necessary.

1.2.1.8.3. The waiver should be monitored to ensure its concurrence with the specified period of time and exception.

1.2.2. OWNERSHIP

1.2.2.1. Executive Owner

1.2.2.1.1. The sponsor of this policy is the Chief Innovation Officers (CIOs) of the government organizations.

Explanatory Notes

The CIOs assume the ownership of the overall security policy and will ensure its maintenance, review, and dissemination.