HPOL#17
Information Security Incident Management

(Version 2.01)

17.0 SCOPE AND OBJECTIVES

The government organization is committed to ensuring that its information assets are protected from unauthorized access, modification and deletion and that information security incidents, events, and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

This policy document addresses the formal incident and event reporting and escalation procedures that should be in place.

17.1 POLICY STATEMENT

17.1.1 **Reporting procedure:**

17.1.1.1 The Government organization should set up a procedure whereby all suspected information security incidents are reported as quickly as possible without any delay, through the appropriate management channels, to the designated information security officer in the organization.

17.1.1.2 The designated officer should inform SLCERT of incidents which cannot be addressed by the organization.

Explanatory notes:

An information security incident can be an occurrence which in itself does not necessarily compromise information security, but which could result in information security being compromised.

17.1.1.3 The Government organization should set up a procedure whereby all security weaknesses in systems and services are reported to the designated officer in the organization.

Explanatory note:

Where there is no procedure to report Information Security weaknesses, there is a possibility that inexperienced staff may try to correct an Information Security weakness in an application program or an operating system and interrupt business critical processing.

Information security incidents should be reported to external entities whenever there is a requirement for compliance with relevant legislation and regulations, or when it is not possible to address the incident internally, by the relevant authorized officers.

It may be necessary to report all significant information security incidents to external entities; for instance, when the organization is not able to address such incidents by itself or due to legal and regulatory obligations, it will be necessary to report to entities such as the SLCERT, regulatory bodies and law enforcement agencies. This should be carried out by the head of the organization.

If there is computer crimes legislation in place, and if such incidents are not reported, the organization may inadvertently be aiding and abetting an offence by not reporting.

17.1.1.4 Employees witnessing information security incidents should report them to the designated information security officer without any undue delay.

Explanatory note:

If a potential information security breach is not reported, an employee and the organization may be implicated in further investigations.

Incidents should not remain un-investigated for unacceptable periods.

17.1.1.5 Breaches of confidentiality should also be reported without undue delay to the designated officer.

.

Explanatory note: Breaches of confidentiality may be a contravention of an employee's employment contract and non-disclosure agreements, if any.

17.1.1.6Where there is a legal requirement to notify relevant authorities of a suspected incident, this should be carried out only by authorized senior management..

17.1.2 Awareness and training:

17.1.2.1Senior Management should ensure that staff, at all levels are provided with awareness programs and training on information security and be made aware that information security is the responsibility of all staff.

Explanatory note:

Staff should be given training and relevant information on a regular basis – if not, there would be a high probability of fraudulent activities not being noticed.

A lack of knowledge may result in highly confidential information about the organization being disclosed to outsiders.

17.1.3 Responding to information security incidents:

17.1.3.1Senior 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.

17.1.3.2 Roles, responsibilities and procedures should be established to ensure quick and effective response to information security incidents.

17.1.3.3 All employees should be alerted to possible threats and specific safeguards to be put in place.

17.1.3.4 Procedures for addressing information security incidents should include

17.1.3.4.1 Procedures for analysis and identification of the cause of the incident.

17.1.3.4.2 Containment of the incident

17.1.3.4.3 Corrective action to prevent recurrence

17.1.3.4.4 Communication with those affected by or involved with recovery from the incident.

17.1.3.4.5 Maintenance of records of corrective action taken.

17.1.3.5 Information relating to information security incidents may be released only if necessary, and then only by authorized persons.

17.1.4 **Investigating information security incidents:**

17.1.4.1Investigation of information security incidents should be carried out by the relevant authorities and by SLCERT, who will call in any other resources required to perform the investigations, if necessary. Law enforcement officials will be informed where an offence is discovered. Where appropriate the criminal discovery process will aid/supplement the SLCERT security incident investigation process.

Explanatory note:

Affected parties must use discretion in deciding whether or not to inform law enforcement agencies of the incident. Informing law enforcement agencies under the following circumstances is recommended:

- Where an incident is found to be a Statutory offence under existing legislation (e.g.:- Computer Crimes Legislation)
- Where there is a threat to national security, public health or safety.
- Where there is a substantial impact on a third party.
- Where there is a legal requirement specific to an industry (e.g. finance) or under national legislation

17.1.4.2. In the investigation of an incident initiated by the Sri Lanka Police, the Police, at their discretion may inform SLCERT when relevant and necessary

Explanatory note:

Handling an incident by untrained personnel may reduce or destroy the evidential value of the relevant information, thereby impeding the digital forensics process. The legislation on Computer Crimes includes provisions for “experts” to assist and take part in the investigative process.

17.1.4.3 In an investigation, evidence shall be collected, recorded, retained and presented in a manner ensuring its integrity and conforming to the rules for evidence and in compliance with the Computer Crimes Legislation and other relevant laws.

Explanatory note:

Investigating an incident should identify its cause and its impact should be appraised in order to prevent its occurring again.

17.1.4.4 During an investigation segregation of duties should be ensured to ensure the integrity of data and information.

17.1.5 **Logging and monitoring:**

17.1.5.1Mechanisms should be in place to formerly record the evidence relating to a suspected information security breach.

17.1.5.2 A database comprising types of information security, potential risks and possible mitigation methods, costs, should be maintained, monitored and updated regularly to help reduce risks and future information security incidents in the organization.

17.1.5.3 Data and information owners and custodians should ensure that inadvertently or otherwise, audit trails should not be modified or deleted.

Explanatory note:

A record would help the organization minimize future breaches of information security and to monitor patterns. The information security policy should also be updated using feedback from such a record. Access to relevant entities such as SLCERT, on reliable information on information security threats within and without the country should also be established