INFORMATION SECURITY INCIDENT MANAGEMENT POLICY

Table of Content

1. Purpose

The purpose of this policy is to ensure that the NIC reacts appropriately to any actual or suspected security incidents relating to information systems and data.

2. Scope

All users shall understand and adopt use of this policy and are responsible for ensuring the safety and security of the Jeevan Rekha software and the information that they use or handle.

3. Objective

The objective of this policy is to ensure that it reacts appropriately to any actual or suspected incidents relating to information systems and information within the custody and infrastructure.

4. Policy Statement

This policy shall be applied as soon as breach of the information systems or data is encountered or suspected to be breached by an adverse event which is likely to lead to a security incident.

An Information Security Incident includes, but is not restricted to, the following:

- The loss or theft of data or information.
- Transfer of data or information to those who are not entitled to receive that information.
- Attempts (either failed or successful) to gain unauthorized access to data or information storage or a computer system.
- Unauthorized changes to information or data or system hardware, firmware, or software characteristics without the organization's knowledge, instruction, or consent.
- Unwanted disruption or denial of service to a system.
- The unauthorized use of the system for the processing or storage of data by any person.
- Intentional or unintentional damage to access control and surveillance systems.
- External or foreign body trying to gain unauthorized access to Jeevan Rekha software information systems.

Responsibilities and Procedures

- Preparation shall involve identification of resources needed for incident handling and having trained individuals ready to respond, and by developing and communicating a formal detection and reporting process.
- Effective, appropriate communication at all levels of an organization shall be implemented for limiting the impact of security events.
- Who can access data relating to an incident under what circumstances and what auditing is required to document the access shall be specified.
- Records of Data retention of non-incident related log data and data preserved during investigation of an incident shall be maintained.
- Computer security professionals shall perform assessments and analysis to determine whether an incident is serious enough to report to law enforcement under the support of IT Act 2000 (amendment 2008)

Reporting Information Security Events

- Designing of an effective means of the detection of incidents shall be implemented using both trained users and trained system administrators, and various technical controls.
- All members of the community shall be trained and comfortable regarding:
    - Procedures for reporting failures, weaknesses, and suspected incidents
    - Methods to recognize and detect problems with security protections
    - How to escalate reporting appropriately
- Technical controls shall be implemented for the automated detection of security events, coupled with possible near real-time reporting, to investigate and initiate immediate responses to incidents.

Reporting Information Security Weaknesses

- Effective system based automated tools are used for analysis to help manage intrusion detection systems and summarize the data.
- Information security events shall be reported through appropriate management channels as quickly as possible.
- Staffs and third party service providers using the organization's information system and services shall note and report any observed or suspected information security weaknesses in

systems or services.

Assessment of incidents and Decision on Information Security Events

- A formal management procedure for incident response, including roles and responsibilities for each aspect of the response shall be documented.
- Information security incidents shall be assessed and it shall be responded to in accordance with the documented procedures.

Response to information security incidents

- Information security incidents shall be responded to in accordance with the documented procedures.
- All the security incidents shall be reported to the concerned authority as per the procedure.

Learning from Information Security Incidents

- Knowledge gained from analyzing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.
- The information must be collated and reviewed on a regular basis by the Information Security team and any patterns or trends identified.
- Any changes to the process made as a result of the Post Incident Review shall be formally noted.

Collection of Evidence

- The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.
- If an incident may require information to be collected for an investigation, strict rules must be adhered to.
- The collection of evidence for a potential investigation shall be approached with care.
- The Internal Audit team shall be contacted immediately for guidance and strict processes must be followed for the collection of evidence.

Rules of evidence

- In case of Jeevan Rekha Software , internal disciplinary matters the necessary evidence will be as per the

requirements of organization's internal procedures. The disciplinary matters will be governed by:

- The terms and conditions of employment or contract.
- Confidentiality agreement with the stake holders.
- Information Security Policy.
- Circulars and instructions issued by Government from time to time.

- In cases where the evidence is to be produced in the court of law, it will be governed by the requirements of the applicable law as listed in the scope above.

- Legal department should be consulted to ensure that the evidence collected is complete and admissible in the court of law.

- In order to ensure that the evidence is admissible and complete, in the internal disciplinary matters or in the court of law

    - The evidence should be complete and unhampered.
    - Implement controls to ensure that the evidence (documentary or electronic) was Secured against unauthorized access and information security policy was consistently implemented across the information assets of Jeevan Rekha.
    - Implement controls to ensure that the process of copying evidence from the Jeevan Rekha Software to a removable media like tape was authorized, controlled and logged.

- The CISO in coordination with the legal department will ensure that the evidence collected is complete and admissible as evidence in the court of law. The evidence collected is stored securely and protected against unauthorized access, modification and destruction.

Admissibility of evidence

- Record / log of all actions during the process of copying the evidence should be created and the process of copying should be witnessed.

- Establish that the logs as available on the system and those copied on the media are the same by using encryption and hashing function.

Quality and completeness of evidence

To ensure that the paper documents and electronic logs are admissible as evidence ,controls need to be implemented and demonstrated as under:

- The paper documents as evidence

    - The original document should be protected against unauthorized access, modification and destruction.
    - The documentation controller should ensure that the documents collected as evidence are secured against unauthorized access, modification or destruction.
    - The paper documents should be archived and retained as per the regulatory requirements and apex body's retention policy.

- The electronic logs as evidence

    - Demonstrate that controls as required by the Information Security Policy have been consistently implemented, maintained and reviewed, on all information assets of Jeevan Rekha Software
    - Audit logs are acceptable evidence as electronic evidence, if secured procedure is applied while collecting it. For establishing accountability of the work done by each user, the audit logs should record the User ID, date and time of logon-logoff, date and time of the event, terminal identification, and records of successful and unsuccessful access attempts and records of resources accessed.
    - Ensure that the date and time stamping of the system generated logs is correct and consistent across all systems. Correct date and time stamping of logs will help analyze and prove the chronology / sequence of activities carried out by the defaulter.
    - Ensure that the access to the logs is restricted. The logs should be protected against unauthorized access, modification and destruction. "Read only" access is permitted for requirements like log analysis, and system auditing. This "read only" access also is based on authorization, logged and recorded securely.
    - Sufficient disk space is always ensured and made available for the logs to be written on the system.
    - CISO/CPM will ensure that in case of outsourced information processing facilities, the logs and other information necessary for investigation and action are copied and stored in a secure manner.

- For information on computer media, record/log of all actions during the copying process should be created.
- Logs of critical systems should be archived and retained as per the regulatory requirements

Virus and worm incident specific procedures

Although virus and worm incidents are very different, the procedures for handling each are very similar, aside from the initial isolation of the system and the time criticality. Worms are not self-replicating and, thus, incidents of this nature are not as time critical as viruses or hacker incidents. Viruses are self-replicating and can spread to hundreds of machines in a matter of minutes; thus, time is a critical factor when dealing with a virus attack. In case, the attack on the systems is

unidentifiable or worm or virus, the procedure for handling virus attacks will hold good and is implemented.

(a). Report to CISO ,TSPOC and MSPOC

Notify the CISO/TSPOC/MSPOC as soon as possible. The CISO/TSPOC/MSPOC will then be responsible for notifying other appropriate personnel.

(b). Identify the problem

Try to identify and isolate the suspected virus or worm-related files and processes. If specific files, which contain virus or worm code, can be identified, then move those files to a safe place or archive them and then remove the infected files. Log all actions.

(c). Inoculate the system(s)

Implement fixes and/or patches to inoculate the system(s) against further attack. Prior to implementing any fixes, it may be necessary to assess the level of damage to the system. If the virus or worm code has been analyzed, then the task of assessing the damage is not very difficult. However, if the offending code has not been analyzed, then it may be necessary to restore the system from backup media.

(d).Perform follow-up analysis.

A follow-up analysis should be done to keep a check on recurrences of the same or similar type of

incident.

Reporting Server Malfunctions

The server malfunctions need to be immediately reported to the SDC Helpdesk

Reporting Application Malfunctions

The application malfunctions need to be immediately reported to the NIC development team.

5. Roles and responsibilities

The Additional Chief Secretary (Finance) is executive owner for this purpose and the members of the team assisting him in incident handling are secondary owners.

i. The Akshaya centres who notice the security incident or malfunction should report it, as quickly as possible to the Akshaya State Centre depending upon the severity of the problem. Akshaya State Centre should report it immediately to NIC/Finance Department . NIC should inform this to CISO/TSPOC/MSPOC.
ii. The CISO will initiate the team of experts to recover from the incident and prevent further damage, track the origin and originator of the incident, complete the forensics process and gather evidence, assist legal and civic bodies in the matter.
iii. The team of experts should take steps to recover from the incident.
iv. CISO should ensure that all employees are made aware of the process of reporting.
v. The Legal Affairs department of Apex body may be contacted for guidelines for collecting evidence.
vi. The CISO/TSPOC/MSPOC shall assess the necessary evidence submitted/collected and review the incident. CISO/TSPOC/MSPOC will review the documentation of the incident, incorporating lessons learnt and improvise / change / introduce new controls to avoid recurrence of such incidents. CISO/TSPOC/MSPOC should report to the Security Forum.
vii. Disciplinary process is to be carried out as per the guidelines detailed in Procedure “Punitive Actions”.

End of Document