Information Security Incident Management Policy

Vishwakarma University

Internal

Title: Incident Management Policy	**Doc No.:**
Approval Date: 18-07-2020	**Review:** Annual
Effective Date: 19-07-2020	**Department:** System and Technology

Ver. No	Release Date	Owner	Approved By	Change details
1.0	19-07-2020	CISO	Vice Chancellor	Initial

Table of Contents

1. Purpose

The purpose of this policy is to ensure that the VU 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 VU's systems and the information that they use or manipulate.

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 to be applied as soon as information systems or data are suspected to be, or are actually affected 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.
- The 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.

- 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 a 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 VU's information systems

4.1. 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 some examination and analysis to determine whether an incident is serious enough to report to law enforcement under the supports of IT Act 2000 (amendment 2008)

4.2. 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 as near real-time reporting as possible, to investigate and initiate immediate responses to problems.

4.3. Reporting Information Security Weaknesses

- An effective approach of tools shall be 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.

4.4. Assessment of 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.

4.5. 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.

4.6. 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 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.

4.7. 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.
- Internal Audit team shall be contacted immediately for guidance and strict processes must be followed for the collection of evidence.

5. Enforcement

- This document applies to all Departments of the VU and third party service providers of the VU who use the VU's IT facilities and equipment, or have access to customer information or the VU's information.
- Any staff found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Reference Documents

- Incident management procedure
- Risk Assessment and Risk Treatment Methodology
- Risk Assessment and Risk Treatment Report
- Business Continuity & Disaster Recovery Plan
- Access Control Policy
- HR IT Procedure

7. Distribution List

- All staffs of Vishwakarma University

8. Acronyms

- VU: Here it refers to Vishwakarma University
- Staff: Here it refers to Teaching Staff/ Non-Teaching Staff/ Office Staff/ Peons
- Information Security Incident is an event that may compromise business operations or threaten business security
- Evidence: the available of facts or information indicating whether a belief or proposition is true or valid.