VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

# FALL SEMESTER 2023-24

# LAB ASSESSMENT -5

**NAME:-** Namit Mehrotra

**Registration Number:-** 21BCE0763

**Course Name:-** Information Security Analysis and Audit Lab BCSE353E

**Slot:-** L57+L58

**Date:-** 13-07-2023

# A) Security incident response plan

## for a higher educational institution

### 1. Introduction

The processes and duties for reacting to security events inside the higher educational institution are outlined in this Security Incident Response Plan. The plan's goal is to reduce the impact of security events, preserve sensitive information, and guarantee that security-related concerns are resolved in a timely and efficient manner.

### 2. Objectives

The objectives of the Security Incident Response Plan are as follows:

- Minimize the impact of security incidents on the institution's systems, networks, and operations.
- Identify and contain security incidents promptly to prevent further compromise.
- Investigate and analyse security incidents to determine the root cause and prevent future occurrences.
- Restore affected systems and services to normal operation as quickly as possible.
- Communicate and collaborate effectively with relevant stakeholders during incident response efforts.

### 3. Definitions

- Security Incident: Any event or action that jeopardizes the confidentiality, integrity, or availability of institutional information, systems, or networks.
- Incident Response Team (IRT): The designated team responsible for managing and coordinating the institution's response to security incidents.
- Incident Response Manager: The individual responsible for overseeing and coordinating the incident response activities.
- System Administrators: Personnel responsible for managing and maintaining the institution's systems and networks.
- Legal Counsel: The legal advisor providing guidance on legal and regulatory matters related to security incidents.
- Communications Officer: The designated person responsible for managing internal and external communication during security incidents.

## 4. Compliance with Policy

- All members of the institution, including staff, students, and contractors, are required to comply with this Security Incident Response Plan.
- Failure to comply with the plan may result in disciplinary actions, including but not limited to, termination, academic penalties, and legal consequences.
- The plan aligns with relevant laws, regulations, and institutional policies regarding incident response and data protection.

## 5. Incident Response Process

### a. Preparation Phase:

• Develop and regularly update the Security Incident Response Plan.

• Establish incident response roles, responsibilities, and contact information.

• Conduct training and awareness programs for the incident response team.

• Implement security monitoring tools and establish incident detection mechanisms.

### b. Detection and Reporting Phase:

• Promptly detect and report security incidents to the Incident Response Manager or designated contact.

• Maintain clear reporting channels for staff and students to report suspected incidents.

### c. Assessment and Response Phase:

• The Incident Response Manager assesses the reported incident, determines its severity, and activates the incident response team.

• The incident response team investigates and contains the incident, following predefined procedures and technical guidelines.

• Determine the scope and impact of the incident, collect evidence, and document findings.

• Communicate with relevant stakeholders, including IT staff, management, affected individuals, and external parties as necessary.

• Implement appropriate mitigation measures to contain and minimize the impact of the incident.

### d. Recovery Phase:

- Restore affected systems, networks, or services to a secure and operational state.

- Conduct post-incident analysis to identify lessons learned and necessary improvements.

- Update incident response procedures and preventive measures based on the lessons learned.

### e. Documentation and Reporting Phase:

- Document all incident response activities, including actions taken, findings, and outcomes.

- Generate incident reports for management, legal purposes, and compliance requirements.

- Maintain incident records securely and in accordance with applicable data protection regulations.

## 6. Communication and Notification

- Establish clear communication channels and protocols for internal and external communication during security incidents.

- Notify relevant stakeholders, including senior management, affected individuals, regulatory bodies, and law enforcement agencies, as required by law and the severity of the incident.

- Coordinate with public relations and legal counsel to manage external communications and media inquiries.

## 7. Training and Awareness

- Conduct regular training and awareness programs for staff, students, and system administrators on security incident reporting and response procedures.

- Promote a culture of security awareness and vigilance throughout the institution.

## 8. Review and Testing

- Conduct periodic reviews and updates of the Security Incident Response Plan to align with emerging threats and changes in the institution's infrastructure.

- Regularly test and evaluate the effectiveness of incident response procedures through tabletop exercises and simulated incident scenarios.

## 9. Appendix

- List of contact information for key personnel and external resources. - Incident response forms, templates, and checklists.
- Incident classification and severity levels.

# B) Security audit report

## 1. Executive Summary

This security audit report evaluates the performance of an information system inside a government entity. The audit includes all elements of security and attempts to raise knowledge of present practises and hazards, minimise risk by reviewing and planning security activities, tighten controls (both human and automated), and assure customer and regulatory compliance.

## 2. Introduction

The goal of this security audit is to assess the efficacy of the government institution's information system security controls and procedures. The audit seeks to uncover possible vulnerabilities, weaknesses, and areas of noncompliance, as well as provide suggestions to improve the system's security posture.

## 3. Scope

The security audit covers the following areas:

- Network security: Assessing the effectiveness of network controls, including firewalls, intrusion detection systems, and network segmentation.

- System security: Evaluating the security configurations, access controls, and patch management practices of the information system.

- Data security: Reviewing data protection mechanisms, encryption practices, and backup and recovery processes.

- Physical security: Assessing the physical access controls, surveillance systems, and environmental safeguards in place.

- Human resources security: Evaluating the effectiveness of security awareness training, user access management, and employee background checks.

- Compliance: Ensuring compliance with relevant customer requirements and regulatory frameworks.

## 4. Methodology

The security audit was conducted using a combination of the following methods:

- Document review: Assessing policies, procedures, and system documentation related to security controls.

- Interviews: Conducting interviews with key personnel to gather information on security practices and processes.

- Technical assessment: Performing vulnerability scanning, penetration testing, and security configuration reviews.

- Physical inspection: Inspecting physical security measures, access control systems, and environmental controls.

## 5. Findings and Recommendations

The security audit identified the following findings:

### a. Network Security:

- Finding: Outdated firewall rules and inadequate network segmentation.

- Recommendation: Regularly review and update firewall rules, implement network segmentation to limit access, and conduct periodic penetration testing to identify vulnerabilities.

### b. System Security:

- Finding: Insufficient patch management practices and weak password policies.

- Recommendation: Implement a robust patch management process, enforce strong password policies, and consider implementing multi- factor authentication.

### c. Data Security:

- Finding: Inadequate data encryption practices and limited backup and recovery procedures.

- Recommendation: Implement data encryption mechanisms for sensitive data, establish regular data backup processes, and test data recovery procedures periodically.

### d. Physical Security:

- Finding: Inconsistent access controls and lack of surveillance coverage.

- Recommendation: Enhance physical access controls with authentication mechanisms, increase surveillance coverage, and conduct regular audits of physical security measures.

### e. Human Resources Security:

- Finding: Inadequate security awareness training and ineffective user access management.

- Recommendation: Develop and deliver comprehensive security awareness training programs, establish proper user access management processes, and perform regular user access reviews.

### f. Compliance:

- Finding: Incomplete compliance with specific customer and regulatory requirements.

- Recommendation: Conduct a gap analysis to identify areas of non- compliance, develop and implement necessary controls to meet customer and regulatory requirements.

## 6. Risk Score Calculation:

To calculate the risk score for each identified finding, we can use a risk scoring matrix that takes into account the likelihood of occurrence and the potential impact of the risk. Here is an example of a risk scoring matrix:

| Likelihood | Impact | Risk Score |
|---|---|---|
| High | High | 9-10 |
| High | Medium | 7-8 |
| High | Low | 5-6 |
| Medium | High | 7-8 |
| Medium | Medium | 4-6 |
| Medium | Low | 2-3 |
| Low | Medium | 2-3 |
| Low | Low | 1 |

Using this matrix, we can assign a risk score to each finding based on the assessed likelihood and impact. The higher the risk score, the greater the urgency in addressing the finding. Here's an example of the risk score calculation for the previously mentioned findings:

### a. Network Security:

- Likelihood: Medium - Impact: Medium
- Risk Score: 4-6

### b. System Security:

- Likelihood: Medium - Impact: Medium
- Risk Score: 4-6

**c. Data Security:**

- Likelihood: Low - Impact: High
- Risk Score: 4-6

**d. Physical Security:**

- Likelihood: Medium - Impact: Medium
- Risk Score: 4-6

**e. Human Resources Security:**

- Likelihood: Medium - Impact: Low
- Risk Score: 2-3

**f. Compliance:**

- Likelihood: Medium - Impact: Low
- Risk Score: 2-3

We may prioritise the discoveries depending on their risk levels by computing risk scores for each discovery and allocating resources appropriately for mitigation and repair actions.

## 7. Conclusion

The security audit identifies opportunities for improvement in the security controls of the government institution's information system. The institution may improve its security posture, decrease risks, and maintain compliance with customer and regulatory obligations by addressing the highlighted issues and adopting the suggested steps.

## 8. Appendices

- Detailed findings and recommendations
- Supporting evidence and documentation
- Audit team members and credentials