Harris McCall
CSIA300
Matt Boehnke
Lab 7

Incident Response Policy

Purpose:

This Incident Response Policy (IRP) outlines XYZ Corporation's approach to managing and responding to security incidents to minimize impact and restore normal operations as swiftly as possible.

Scope:

The IRP applies to all information systems, network resources, employees, contractors, and third-party partners involved in the operation of XYZ Corporation.

Policy:

XYZ Corporation shall establish and maintain an incident response program to identify, manage, record, and analyze security incidents in a timely and effective manner, as recommended by NIST SP 800-61 and in accordance with ISO/IEC 27035 principles.

Roles and Responsibilities:

- Incident Response Team (IRT): Responsible for executing the IRP, managing incidents through their lifecycle, and communicating with stakeholders.
- Security Officer: Provides oversight for the incident response program and advises senior management.
- IT Staff: Assist in the technical support and analysis of incidents.
- Employees: Report suspected incidents promptly according to the procedures outlined in section 6.

Incident Classification:

Following guidelines set in ISO/IEC 27035, incidents shall be categorized by severity levels (e.g., Low, Medium, High, Critical) based on factors such as impact, scale, and sensitivity of the affected data.

Incident Reporting:

All potential security incidents must be reported immediately to the IRT through established reporting channels such as an incident reporting hotline, email, or an incident tracking system.

Incident Response Procedures:

The IRT shall follow structured procedures that include:

- Identification: Determine if an incident has occurred and assess its potential impact.
- Containment: Isolate affected systems to prevent further damage.
- Eradication: Identify and remove the root cause and vulnerabilities.
- Recovery: Restore systems to normal operations and confirm that they are no longer compromised.
- Lessons Learned: Review each incident to improve future response and prevent recurrence.

Review and Audit:

The IRP will be reviewed and audited at least annually or after major incidents to ensure effectiveness and to adapt to new threats, incorporating lessons learned, and reflecting organizational changes in accordance with NIST SP 800-61 and ISO/IEC 27035.

Disaster Recovery Policy

Purpose:

The purpose of this Disaster Recovery Policy (DRP) is to establish the framework for XYZ Corporation's recovery from a major disaster or significant event that affects its IT infrastructure and operations.

Scope:

This policy applies to all IT systems, networks, and data essential to the operation of XYZ Corporation, including all locations, technical staff, and third parties involved in the IT operations.

Policy:

It is the policy of XYZ Corporation to maintain a comprehensive disaster recovery plan that is regularly reviewed, updated, and tested to ensure it aligns with business requirements and adheres to relevant standards such as NIST SP 800-34 and ISO/IEC 27031.

Roles and Responsibilities:

- Disaster Recovery Manager: Oversees the DRP, leads recovery efforts, and communicates with executive management.
- IT Department: Responsible for restoring IT capabilities and for maintaining up-to-date system backups.
- HR and Communications: Ensure that all staff are informed about the DRP and their individual roles.

Recovery Strategies:

Recovery strategies shall ensure the timely restoration of IT systems and operations and may include redundant systems, data backups, alternative processing site agreements, and prioritization of critical systems.

Implementation Steps:

The implementation of the DRP includes:

1. Activation: Upon declaration of a disaster, the DRP shall be activated.
2. Notification and Assembly: Staff responsible for executing the DRP shall be notified and convened promptly.
3. Damage Assessment: Evaluate the extent of the damage and its impact on operations.
4. Execution: Commence recovery operations in accordance with the prioritized critical systems list.
5. Restoration: Systems and operations are restored to normal levels as outlined in the recovery strategies.

Testing and Maintenance:

The DRP will be tested at least annually to ensure its effectiveness in a real-life scenario. The plan shall also be maintained and updated to reflect changes in IT infrastructure, business processes, and lessons learned from tests and real incidents.

Business Continuity Policy

Purpose:

This Business Continuity Plan (BCP) outlines the process that XYZ Corporation will follow to ensure the continuation of critical business functions in the event of a significant business disruption or disaster.

Scope:

The BCP encompasses all critical business functions and processes, IT systems, personnel, and facilities. It covers scenarios such as natural disasters, technological failures, cyberattacks, and other events that could interrupt business operations.

Policy:

XYZ Corporation is committed to maintaining a BCP in accordance with NIST SP 800-34 and ISO 22301 standards, which will be reviewed and updated on a regular basis, to ensure minimum disruption to business operations and services to customers in the event of an incident.

Roles and Responsibilities:

- Business Continuity Manager: Develops, maintains, and implements the BCP.
- Senior Management: Ensures the BCP is adequately resourced and integrated into company culture.
- Department Heads: Identify critical business functions within their areas and develop departmental continuity strategies.
- All Employees: Familiarize themselves with the BCP and take part in training and exercises.

Business Impact Analysis:

This analysis identifies and evaluates the potential effects of disruptions to business operations. It will pinpoint the most critical business functions and processes, setting recovery time objectives (RTOs) and recovery point objectives (RPOs).

Continuity Strategies:

Continuity strategies will be developed to address the restoration of business operations within an acceptable timeframe after a disruption. This may include alternative business practices, reciprocal agreements with third parties, diversification of resources, or temporary relocation of business processes.

Training and Awareness:

All staff must be trained on their specific roles and responsibilities in the BCP. Regular awareness programs and training exercises will be conducted to ensure that all employees are prepared and that the BCP is effective.