Incident Management Policy Template

Document Control Information

- **Document Title:** Incident Management Policy
- **Document Version:** 1.0
- **Last Updated:** [DATE]
- **Document Owner:** [ROLE/NAME]
- **Approved By:** [ROLE/NAME]
- **Next Review Date:** [DATE]

1. Introduction

1.1 Purpose

This Incident Management Policy establishes [ORGANIZATION NAME]'s approach to managing information security incidents in accordance with ISO 27001:2022 requirements. It provides a framework for the detection, reporting, assessment, response, and learning from information security incidents to minimize their impact and reduce the risk of similar incidents occurring in the future.

1.2 Scope

This policy applies to: - All information security incidents affecting [ORGANIZATION NAME]'s information assets - All employees, contractors, consultants, temporary staff, and other workers - All information systems, networks, applications, and data owned or managed by the organization - All locations from which organizational information is accessed - All third parties that access or manage organizational information systems or data

1.3 Policy Statement

[ORGANIZATION NAME] is committed to: - Promptly detecting and responding to information security incidents - Minimizing the impact of incidents on business operations, assets, and stakeholders - Preventing the escalation of incidents and reducing recovery time and costs - Learning from incidents to improve security controls and prevent recurrence - Complying with legal, regulatory, and contractual incident reporting requirements - Maintaining appropriate documentation of incidents and responses

2. Incident Classification and Prioritization

2.1 Incident Definition

An information security incident is defined as a single event or series of unwanted or unexpected events that have a significant probability of compromising business operations or threatening information security. Examples include: - Unauthorized access to systems or data - Malware infections - Data breaches or leaks - Denial of service attacks - Physical security breaches affecting information assets - Loss or theft of equipment containing sensitive information - Misuse of information systems or data

2.2 Incident Classification

Incidents shall be classified based on the type of security breach:

2.2.1 Confidentiality Breach

- Unauthorized disclosure of information
- Data leakage
- Inappropriate access to sensitive information
- Loss or theft of information assets

2.2.2 Integrity Breach

- Unauthorized modification of data
- Corruption of information
- System or data tampering
- Injection of false information

2.2.3 Availability Breach

- Denial of service
- System or service outage
- Loss of access to information
- Destruction of equipment or data

2.3 Incident Prioritization

Incidents shall be prioritized based on:

2.3.1 Severity Levels

- **Critical**: Severe impact on critical systems or data; significant business disruption; potential legal or regulatory implications; widespread effect
- **High**: Significant impact on important systems or data; limited business disruption; potential for escalation if not addressed quickly
- **Medium**: Moderate impact on systems or data; minimal business disruption; contained to specific systems or departments
- **Low**: Minor impact on non-critical systems or data; no business disruption; easily contained and resolved

2.3.2 Prioritization Factors

- Impact on business operations
- Sensitivity and criticality of affected information
- Number of systems or users affected
- Potential for damage or loss
- Regulatory or legal implications
- Reputational impact
- Spread or growth rate of the incident

3. Incident Response Organization

3.1 Incident Response Team

An Incident Response Team (IRT) shall be established with representatives from: - Information Security - IT Operations - Legal - Human Resources - Communications/ Public Relations - Business Units (as needed) - Executive Management (for critical incidents)

3.2 Roles and Responsibilities

3.2.1 Incident Response Manager

- Coordinate incident response activities
- Determine incident severity and priority
- Allocate resources for incident handling
- Escalate incidents when necessary
- Report to senior management
- Ensure proper documentation

3.2.2 Technical Response Team

- Investigate technical aspects of incidents
- Contain and eradicate threats
- Restore affected systems and data
- Collect and preserve evidence
- Implement technical countermeasures
- Document technical findings

3.2.3 Communications Coordinator

- Manage internal communications about incidents
- Coordinate external communications when necessary
- Liaise with public relations for significant incidents
- Ensure stakeholders are appropriately informed
- Prepare communication templates

3.2.4 Legal Advisor

- Provide guidance on legal implications
- Advise on regulatory reporting requirements
- Ensure evidence collection meets legal standards
- Review communications for legal compliance
- Manage interactions with law enforcement

3.2.5 All Staff

- Report suspected security incidents promptly
- Cooperate with incident investigations
- Follow incident response procedures
- Preserve evidence when possible
- Maintain confidentiality about incidents

4. Incident Response Lifecycle

4.1 Preparation

- Develop and maintain incident response procedures
- Train staff on incident detection and reporting
- Establish and test communication channels
- Prepare incident response tools and resources
- Conduct regular incident response exercises
- Maintain contact information for key personnel

4.2 Detection and Reporting

4.2.1 Detection Methods

- Security monitoring systems
- Intrusion detection/prevention systems
- Anti-malware alerts
- Log analysis
- User reports
- Third-party notifications
- Physical security alerts

4.2.2 Reporting Procedures

- All staff shall report suspected incidents immediately
- Reports shall be made to [SPECIFY CONTACT METHOD]
- Reports shall include:
  - Date and time of discovery
  - Nature of the incident
  - Systems, data, or services affected
  - Actions taken so far
  - Contact information of the reporter
- Anonymous reporting shall be available
- Reports shall be acknowledged and tracked

4.3 Assessment and Triage

- Initial assessment shall be conducted promptly
- Incident classification and prioritization shall be determined
- Appropriate response team members shall be notified
- Need for escalation shall be evaluated
- Initial containment actions shall be identified
- Response strategy shall be developed

4.4 Containment

- Immediate actions shall be taken to limit incident impact
- Short-term containment shall focus on isolating affected systems
- Long-term containment shall address underlying vulnerabilities
- Containment actions shall be documented
- Business impact of containment actions shall be considered
- Management approval shall be obtained for high-impact containment actions

4.5 Investigation and Evidence Collection

4.5.1 Investigation Process

- Determine the scope and impact of the incident
- Identify the cause and attack vectors
- Document the timeline of events
- Identify affected systems and data
- Determine if sensitive or personal data was compromised
- Assess regulatory and compliance implications

4.5.2 Evidence Collection

- Evidence shall be collected following forensic principles
- Chain of custody shall be maintained
- Evidence shall be secured and preserved
- Evidence collection shall be documented
- External forensic experts shall be engaged when necessary
- Legal requirements for evidence shall be followed

4.6 Eradication

- Root causes shall be identified and addressed
- Malware and other threats shall be removed
- Vulnerabilities shall be patched or mitigated
- Compromised accounts shall be reset
- Systems shall be hardened against similar attacks
- Eradication actions shall be verified

4.7 Recovery

- Systems and data shall be restored to normal operation
- Restoration shall be done from clean backups when possible
- Restored systems shall be validated before returning to production
- Additional monitoring shall be implemented for recovered systems
- Users shall be notified when services are restored
- Recovery actions shall be documented

4.8 Post-Incident Activities

4.8.1 Lessons Learned

- Post-incident review meetings shall be conducted

- Root causes shall be analyzed
- Effectiveness of response shall be evaluated
- Improvements to security controls shall be identified
- Incident response procedures shall be updated as needed
- Lessons learned shall be documented and shared appropriately

4.8.2 Documentation

- Comprehensive incident reports shall be prepared
- Reports shall include:
    - Incident description and timeline
    - Actions taken
    - Impact assessment
    - Root cause analysis
    - Recommendations for prevention
- Documentation shall be retained according to retention policies

5. Communication and Reporting

5.1 Internal Communication

- Regular updates shall be provided to stakeholders
- Communication shall be clear, timely, and appropriate
- Communication channels shall be secure
- Need-to-know principles shall be applied
- Escalation procedures shall be followed for significant incidents

5.2 External Communication

5.2.1 Customer and Partner Communication

- Affected customers and partners shall be notified when appropriate
- Communications shall be approved by legal and management
- Communications shall be clear, factual, and timely
- Support resources shall be provided to affected parties
- Follow-up communications shall be provided as needed

5.2.2 Public Communication

- Public statements shall be approved by senior management
- Communications shall be coordinated with public relations
- Only authorized spokespersons shall communicate with media
- Communications shall be consistent and accurate

- Social media shall be monitored during public incidents

5.3 Regulatory Reporting

- Incidents requiring regulatory reporting shall be identified
- Reporting timeframes shall be followed
- Reports shall include required information
- Legal counsel shall review regulatory reports
- Regulatory communications shall be documented

6. Special Incident Types

6.1 Data Breach Incidents

- Data breaches shall be handled according to the Data Breach Response Procedure
- Privacy regulations shall be followed for personal data breaches
- Impact assessment shall determine notification requirements
- Affected individuals shall be notified according to legal requirements
- Remediation shall include measures to prevent similar breaches

6.2 Ransomware Incidents

- Ransomware response shall follow the Ransomware Response Procedure
- Systems shall be isolated to prevent spread
- Backups shall be verified before restoration
- Law enforcement shall be notified as appropriate
- Payment of ransom shall require executive approval
- Recovery shall prioritize critical business functions

6.3 Insider Threat Incidents

- Insider threats shall be handled with additional confidentiality
- Human Resources shall be involved in the response
- Evidence collection shall be thorough and legally sound
- Access shall be managed to prevent further damage
- Investigation shall follow employment laws and policies

7. Testing and Improvement

7.1 Incident Response Testing

- Incident response procedures shall be tested regularly

- Tests shall include:
  - Tabletop exercises
  - Simulated incidents
  - Technical drills
  - Full-scale exercises
- Test results shall be documented and analyzed
- Improvements shall be implemented based on test results

7.2 Continuous Improvement

- Incident response capabilities shall be regularly assessed
- Metrics shall be collected and analyzed
- Industry best practices shall be monitored
- Threat intelligence shall inform improvements
- Feedback shall be collected from incident responders
- Procedures shall be updated based on lessons learned

8. Training and Awareness

8.1 Incident Response Team Training

- IRT members shall receive specialized training
- Training shall be refreshed annually
- Training shall cover:
  - Incident response procedures
  - Investigation techniques
  - Evidence handling
  - Communication protocols
  - Tools and resources
- Certifications shall be encouraged where appropriate

8.2 General Staff Awareness

- All staff shall receive incident reporting awareness
- Training shall cover:
  - How to recognize security incidents
  - How to report incidents
  - Initial response actions
  - Preservation of evidence
- Awareness materials shall be regularly updated
- Simulated phishing and other awareness tests shall be conducted

9. Related Documents

- Information Security Policy
- Data Breach Response Procedure
- Business Continuity Plan
- Disaster Recovery Plan
- Evidence Handling Procedure
- Incident Response Playbooks
- [LIST OTHER RELEVANT POLICIES AND PROCEDURES]

10. Approval

This Incident Management Policy is approved by:

Name: _______________________ Position: _____________________ Date: ________________________ Signature: ____________________