Incident Response Policy for Network Security

Version 1.2 | Last Updated: March 1, 2025

1. Purpose

This policy establishes a structured approach to detecting, responding to, mitigating, and recovering from security incidents affecting the corporate network. It ensures a swift and effective response to minimize damage, reduce recovery time, and prevent future occurrences. The policy is reviewed quarterly or as needed based on emerging threats to ensure its effectiveness.

2. Scope

This policy applies to all employees, contractors, third-party vendors, and any authorized users who:

- Access corporate networks, systems, or data.
- Use personal or corporate devices to connect to internal or cloud-based company resources.
- Are responsible for managing, monitoring, or securing IT infrastructure and applications.

This policy covers all network-related security incidents, including but not limited to unauthorized access, malware infections, data breaches, denial-of-service attacks, and insider threats.

3. Incident Classification

Security incidents are classified into four categories based on their severity:

3.1. Low-Risk Incidents (Tier 1)

- Minor security violations with no direct impact on operations
- Examples:
    - Isolated failed login attempts below threshold
    - Minor policy violations (e.g., accessing non-business websites)
    - Attempted access to non-sensitive blocked resources
    - Isolated malware detections that were successfully quarantined
- Response Time: Within 24 hours

3.2. Medium-Risk Incidents (Tier 2)

- Potential threats that could escalate if not addressed promptly
- Examples:
  - Multiple failed login attempts from the same source
  - Unauthorized device connections to the network
  - Suspicious network traffic patterns or data exfiltration attempts
  - Detection of potentially unwanted applications
  - Non-critical system performance issues indicating possible security problems
- Response Time: Within 8 hours

3.3. High-Risk Incidents (Tier 3)

- Direct threats to network security requiring immediate attention
- Examples:
  - Confirmed malware infections not automatically remediate
  - Compromised user credentials or privileged accounts
  - Unauthorized access to sensitive data
  - Targeted phishing attacks against specific employees
  - Successful exploitation of system vulnerabilities
- Response Time: Within 2 hours

3.4. Critical Incidents (Tier 4)

- Major security breaches causing operational disruptions, financial loss, or regulatory violations
- Examples:
  - Ransomware attacks affecting multiple systems
  - Advanced Persistent Threats (APTs) detected within the network
  - Major data breaches involving customer or sensitive corporate information
  - Widespread system outages due to security incidents

    - Coordinated cyber attacks on the organization

- Response Time: Within 15 minutes

4. Incident Response Team Structure

4.1. Core Incident Response Team

- **Incident Response Manager**: Oversees the entire incident response process
- **Network Security Specialists**: Handle technical investigation and containment
- **System Administrators**: Assist with system recovery and technical remediation
- **Forensic Analysts**: Perform detailed analysis of incidents and evidence collection

4.2. Extended Response Team (for High-Risk and Critical Incidents)

- **Chief Information Security Officer (CISO)**: Strategic oversight and stakeholder communication
- **Legal Counsel**: Handles legal implications and regulatory compliance
- **Public Relations**: Manages external communications when needed
- **Human Resources**: Addresses incidents involving employee misconduct
- **Executive Leadership**: Informed and involved in critical incident decisions

5. Incident Response Phases

5.1. Identification

- Users must report any suspected security incidents immediately to the IT Security Team.
- Automated monitoring tools, including AI-driven threat detection, will log and detect unusual network activities.
- Security alerts from the following sources will be analyzed:
    - Intrusion Detection/Prevention Systems (IDS/IPS)
    - Security Information and Event Management (SIEM) system
    - Firewall and network device logs
    - Endpoint Detection and Response (EDR) solutions
    - Data Loss Prevention (DLP) alerts

    - Cloud security platforms

5.2. Containment

5.2.1. Immediate Containment

- For minor incidents, network access may be temporarily restricted to prevent escalation.
- High-risk and critical incidents require immediate isolation of affected devices, accounts, or services.
- Unauthorized access attempts will trigger automatic session termination and user verification.
- Potentially compromised accounts will be temporarily locked and require identity verification.

5.2.2. Short-term Containment

- Affected systems will be isolated using network segmentation or removal from the network.
- Temporary security controls will be implemented to prevent incident spread.
- Access privileges will be adjusted based on the principle of least privilege.

5.2.3. Long-term Containment

- Patching and securing systems before returning to production.
- Implementation of additional monitoring for affected systems.
- Hardening of systems based on the attack vector identified.

5.3. Eradication

- IT Security will analyze the root cause through forensic investigation.
- Malware and unauthorized software will be removed using approved security tools.
- Compromised credentials will be reset and additional authentication factors may be required.
- Vulnerability scanning and penetration testing will be conducted to verify remediation.

- For network-based attacks, firewall rules and intrusion prevention system (IPS) policies will be updated.
- Advanced threats may require:
  - Complete system reimaging
  - Application of security patches and updates
  - Removal and replacement of compromised hardware if necessary

5.4. Recovery

- Affected systems will be restored from known-good backups when necessary.
- Restoration priority will be based on business criticality as defined in the Business Continuity Plan.
- Before reinstating systems, the following must occur:
  - Security patches must be applied
  - Passwords and access credentials must be reset
  - Multi-factor authentication must be enforced
  - Security configurations must be verified
- Post-recovery verification will include:
  - Security scans to confirm threat removal
  - Functionality testing to ensure system operation
  - Continuous monitoring for 72 hours minimum after recovery
- Employees involved in an incident may be required to undergo security training if human error contributed to the breach.

5.5. Lessons Learned & Reporting

- A detailed post-incident report will be compiled within 5 business days, including:
  - Incident timeline and chronology
  - Attack vectors and methodology
  - Impact assessment (operational, financial, reputational)
  - Effectiveness of the response

    - Recommendations for prevention of similar incidents

- Security posture improvements will be implemented based on findings.
- Existing controls will be evaluated and enhanced as necessary.
- If necessary, legal and compliance teams will be engaged for regulatory reporting.
- Annual tabletop exercises will be conducted to simulate different attack scenarios.

6. Incident Reporting & Escalation

6.1. Employee Responsibilities

All users must report security incidents via:

- 📧 Email: security-report@[companydomain].com
- 📞 Phone: [Company Security Hotline]
- 🌐 Incident Reporting Portal: [Company IT Security Portal]
- In person to IT Security personnel for urgent matters

When reporting, users should provide:

- Date and time of the incident
- Systems, data, or applications involved
- Description of the unusual behavior or security concern
- Any error messages or suspicious communications received
- Actions taken after discovering the incident

Failure to report security incidents in a timely manner may result in disciplinary action.

6.2. IT Security Team Responsibilities

- Acknowledge receipt of all security incident reports within 30 minutes.
- Provide initial response within 15 minutes for critical incidents and 2 hours for high-risk incidents.
- Maintain comprehensive incident response logs in the security incident management system.
- Coordinate with external security firms when specialized expertise is required.

- Communicate incident status updates to stakeholders based on the communication plan.
- Document all investigative steps, findings, and remediation actions.

6.3. Escalation Procedures

- Incidents will be escalated based on the following criteria:
    - If the incident cannot be contained within 4 hours
    - If the incident affects critical business systems
    - If the incident involves sensitive data or regulatory concerns
    - If the incident impacts more than 10% of corporate users
    - If the incident appears to be part of a targeted attack

6.3.1. Escalation Path

1. Tier 1: IT Security Analyst
2. Tier 2: IT Security Manager
3. Tier 3: CISO or IT Director
4. Tier 4: Executive Leadership and Legal Team

6.3.2. External Escalation

- Law enforcement involvement will be determined by the CISO in consultation with legal counsel.
- Regulatory notifications will be handled by the compliance team within required timeframes.
- Customer notifications will follow the Data Breach Notification Procedure when applicable.

6.3.3. Communication Protocols

- Employees and key stakeholders will be notified through:
    - Company-wide email for general awareness
    - SMS alerts for immediate concerns
    - Internal security dashboard for ongoing updates

    - Emergency notification system for critical incidents

7. Documentation & Evidence Handling

7.1. Required Documentation

- All incidents must be documented in the Incident Response Management System.
- Documentation must include:
    - Incident ID and classification
    - Discovery and reporting information
    - Systems and data affected
    - Remediation actions taken
    - Resolution details and timeline
    - Evidence collected and preserved

7.2. Evidence Collection and Preservation

- Evidence must be collected following digital forensic best practices:
    - Maintain chain of custody documentation
    - Create forensic images when appropriate
    - Capture logs, memory dumps, and network captures as needed
    - Document all evidence collection steps
- Evidence retention periods:
    - Low-risk incidents: 3 months
    - Medium-risk incidents: 1 year
    - High-risk and critical incidents: 7 years or as required by legal/regulatory requirements

8. Enforcement & Compliance

8.1. Policy Compliance

- Quarterly security awareness training will include incident response procedures.
- Annual incident response drills and tabletop exercises will be conducted for all IT staff.

- Simulation exercises for phishing and social engineering will be performed regularly.
- Non-compliance with this policy may result in:
  - Verbal warning for first minor offense
  - Written warning for repeated offenses
  - Disciplinary action up to and including termination for serious violations

8.2. Policy Governance

- The IT Security Team will review and update this policy quarterly.
- All changes to this policy must be approved by the CISO and IT Governance Committee.
- Exemptions to policy requirements must be documented and approved by the CISO.

9. Integration with Other Policies

This policy works in conjunction with:

- Business Continuity Plan
- Disaster Recovery Plan
- Data Classification Policy
- BYOD Security Policy
- Acceptable Use Policy
- Data Breach Notification Procedure

10. Policy Acknowledgment & Agreement

I, [Employee Name], acknowledge that I have read, understood, and agree to comply with the Network Security Incident Response Policy.

Employee Signature: ___________________ Date: _______________