# INCIDENT RESPONSE PLAN

Version 2.1 | Effective Date: March 10, 2025 | Classification: CONFIDENTIAL

## 1. INTRODUCTION

This Incident Response Plan establishes the procedures for effectively identifying, responding to, and recovering from security incidents that may affect TNO's information systems, data, and operations. This plan aims to minimize damage and reduce recovery time and costs when security incidents occur.

## 2. SCOPE

This plan applies to all security incidents involving TNO's information systems, networks, data, and resources, whether hosted internally, in the cloud, or managed by third parties. It covers all employees, contractors, and partners who use or have access to TNO information resources.

## 3. INCIDENT RESPONSE TEAM

### 3.1 Team Structure

The Incident Response Team (IRT) consists of the following roles:

1. \*\*Incident Response Manager\*\*: Oversees the entire incident response process

2. \*\*Security Analysts\*\*: Perform technical investigation and analysis

3. \*\*System Administrators\*\*: Assist with containment and recovery actions

4. \*\*Network Engineers\*\*: Monitor and analyze network traffic

5. \*\*Legal Counsel\*\*: Advises on legal implications and requirements

6. \*\*Communications Officer\*\*: Manages internal and external communications

7. \*\*Executive Sponsor\*\*: Provides executive-level support and decision-making

8. \*\*Human Resources Representative\*\*: Handles personnel-related aspects

### 3.2 Contact Information

The incident response team shall be notified immediately upon discovery of a security incident through the following channels:

- \*\*Emergency Hotline\*\*: +31-20-555-7777 (24/7)

- \*\*Email\*\*: incident@tno-example.com

- \*\*Security Operations Center\*\*: Extension 5555 (internal)

- \*\*Security Portal\*\*: https://security.tno-example.com/report-incident

## 4. INCIDENT CLASSIFICATION

### 4.1 Incident Types

1. \*\*Data Breach\*\*: Unauthorized access, disclosure, or exfiltration of sensitive data

2. \*\*Malware Infection\*\*: Systems compromised by viruses, ransomware, or other malicious code

3. \*\*Denial of Service\*\*: Attacks that impair or prevent normal system operation

4. \*\*Unauthorized Access\*\*: Illegal or unauthorized system access

5. \*\*Social Engineering\*\*: Phishing, impersonation, or manipulation attacks

6. \*\*Physical Security\*\*: Unauthorized physical access or theft of assets

7. \*\*Insider Threat\*\*: Malicious actions by authorized users

8. \*\*Third-Party Breach\*\*: Security incidents at vendors or partners affecting TNO

### 4.2 Severity Levels

Incidents shall be categorized according to the following severity levels:

1. \*\*Critical (Level 1)\*\*

- Significant impact on critical systems or sensitive data

- Potential for significant financial or reputational damage

- Regulatory reporting likely required

- Examples: Large-scale data breach, ransomware affecting critical systems

2. \*\*High (Level 2)\*\*

- Limited impact on critical systems or sensitive data

- Potential for moderate financial or reputational damage

- Examples: Compromised administrator account, malware on multiple systems

3. \*\*Medium (Level 3)\*\*

- Minimal impact on non-critical systems

- Limited exposure of non-sensitive data

- Examples: Isolated malware infection, successful phishing attack without evidence of further compromise

4. \*\*Low (Level 4)\*\*

- No immediate impact on systems or data

- Suspicious activities or attempted attacks

- Examples: Unsuccessful attacks, suspicious emails, minor policy violations

## 5. INCIDENT RESPONSE PROCESS

### 5.1 Preparation

1. Maintain current network diagrams and system documentation

2. Conduct regular security training for all employees

3. Perform regular backup and recovery testing

4. Establish and test communication protocols

5. Maintain incident response toolkit and resources

6. Document standard operating procedures for common incidents

### 5.2 Detection and Reporting

1. Monitor security events through SIEM and other security tools

2. Enable logging on all critical systems

3. Train employees to recognize and report suspicious activities

4. Establish clear channels for incident reporting

5. Review alerts and reports to identify potential incidents

### 5.3 Assessment and Triage

1. Verify that the incident is genuine

2. Determine the incident type and severity

3. Identify affected systems and data

4. Estimate potential impact and risk

5. Determine the appropriate response level

6. Activate the necessary Incident Response Team members

### 5.4 Containment

1. Isolate affected systems to prevent further spread

2. Block malicious IP addresses or domains

3. Disable compromised accounts

4. Implement emergency access controls

5. Preserve evidence for later analysis

6. Document all containment actions

### 5.5 Eradication

1. Remove malware and other unauthorized code

2. Patch vulnerabilities that were exploited

3. Reset compromised credentials

4. Verify that all malicious components have been removed

5. Scan systems to ensure cleanliness

6. Document all eradication actions

### 5.6 Recovery

1. Restore systems from clean backups

2. Verify system integrity and functionality

3. Implement additional security controls

4. Gradually return systems to production

5. Monitor systems closely for signs of recurring issues

6. Document all recovery actions

### 5.7 Post-Incident Activities

1. Conduct a formal post-incident analysis

2. Document lessons learned

3. Implement improvements to prevent similar incidents

4. Update incident response procedures as needed

5. Conduct follow-up training if necessary

6. Share applicable threat intelligence with trusted partners

## 6. EVIDENCE HANDLING

Evidence must be preserved according to the following procedures:

1. \*\*Collection\*\*:

- Use write-blockers when collecting evidence from storage media

- Capture system memory before powering down systems

- Take screenshots of suspicious activities

- Preserve original log files

2. \*\*Documentation\*\*:

- Maintain detailed chain of custody records

- Document who collected evidence, when, and how

- Record all actions taken with the evidence

- Create detailed descriptions of all evidence items

3. \*\*Storage\*\*:

- Store digital evidence in encrypted form

- Maintain at least two copies of all evidence

- Store physical evidence in secured, access-controlled areas

- Label all evidence properly with case number, date, and collector

4. \*\*Preservation\*\*:

- Never analyze original evidence directly

- Create forensic copies for analysis

- Verify integrity using cryptographic hashes

- Maintain evidence for the required retention period

## 7. COMMUNICATION PLAN

### 7.1 Internal Communication

1. Initial notification to management within 1 hour of incident confirmation

2. Regular status updates to stakeholders

3. Detailed briefings for executives and board members as needed

4. Employee notifications when necessary

5. Use secure communication channels for sensitive discussions

### 7.2 External Communication

1. Customer notifications as required by law or contracts

2. Regulatory notifications within required timeframes

3. Law enforcement contact for criminal activities

4. Public statements approved by legal and executive team

5. Coordination with PR team for media inquiries

## 8. REGULATORY REQUIREMENTS

1. GDPR breach reporting within 72 hours to supervisory authorities

2. Industry-specific reporting requirements

3. Documentation of incident details and response actions

4. Communication with affected data subjects when required

5. Cooperation with authorities during investigations

## 9. TESTING AND MAINTENANCE

1. Conduct tabletop exercises quarterly

2. Perform full-scale simulations annually

3. Update contact information monthly

4. Review and update the plan at least annually

5. Train new Incident Response Team members

## 10. APPROVAL AND REVIEW

This Incident Response Plan shall be reviewed annually and updated as needed to reflect changes in technology, threats, and organizational structure.

APPROVED BY:

Elizabeth Reynolds, Chief Information Security Officer

Date: March 10, 2025