**Disclaimer:**

This Incident Response Plan template is provided for general informational purposes only. It is not a substitute for professional advice, and users should adapt it to their specific needs and circumstances. While this template is based on best practices, L2 Cyber Security Solutions make no warranties or guarantees regarding its effectiveness or suitability for any particular situation. Users are responsible for ensuring the accuracy and completeness of the plan for their organisation. This template does not constitute legal advice, and users should consult with legal counsel for their specific legal needs. Incident response best practices evolve, and users are encouraged to stay updated on industry standards. It is crucial to regularly test and revise this plan to ensure its effectiveness.

**[Your Organisation Logo]**

**[Organisation Name]**

Incident Response Plan (IRP)

Version: 1.0

Date: **[Date]**

Contents

[1. Introduction 3](#_Toc161831955)

[2. Incident Response Team 3](#_Toc161831956)

[3. Preparation 3](#_Toc161831957)

[4. Incident Response Procedures 5](#_Toc161831958)

[5. Investigation and Analysis 7](#_Toc161831959)

[6. Documentation and Reporting 7](#_Toc161831960)

[7. Remediation and Recovery 7](#_Toc161831961)

[8. Lessons Learned and Post-Incident Review 7](#_Toc161831962)

[9. Legal and Regulatory Compliance 7](#_Toc161831963)

[10. Plan Maintenance and Training 7](#_Toc161831964)

[11. References and Appendices 7](#_Toc161831965)

[Appendix (a) – Incident Reporting Form: 8](#_Toc161831966)

[Appendix (b) – Incident Log Template: 11](#_Toc161831967)

[Appendix (c) – Post Incident Review Template: 12](#_Toc161831968)

[Appendix (d) – Playbooks: 14](#_Toc161831969)

[Appendix (e) – Incident Response Plan Test Scenarios: 15](#_Toc161831970)

[Appendix (f) – Evidence Preservation Guidelines 17](#_Toc161831971)

# 1. Introduction

Purpose of the Incident Response Plan

Scope and Applicability

Goals and Objectives

#

# 2. Incident Response Team

Roles and Responsibilities

Contact Information:

| **Role** | **Name** | **Contact Information** |
| --- | --- | --- |
| Incident Team Lead | [Name] | Email, Phone |
| Technical & SMEs | [Name] | Email, Phone |
| Data Protection & Legal | [Name] | Email, Phone |
| Communication Lead | [Name] | Email, Phone |
| Human Resources | [Name] | Email, Phone |

#

# 3. Preparation

Identify and document critical assets:

| **Asset** | **Description** |
| --- | --- |
| Customer data | Where is it stored, how is it protected, are there backups? |
| Financial data | Where is it stored, how is it protected, are there backups? |
| IT Systems | Where is it stored, how is it protected, are there backups? |
| Sensitive data | Where is it stored, how is it protected, are there backups? |
| Personnel | Who are they and why are they important? |
| Other | What are they and why are they important? |

Define Incident Categories:

| **Category** | **Description** |
| --- | --- |
| Unauthorised Access | Unauthorised access to systems or data |
| Malware | Malicious software detected or suspected |
| Data Breach | Unauthorised access or exposure of data |
| Denial of Service | Disruption of network or system availability |
| Insider Threat | Suspicious activities by internal users |
| Other | Define other incident categories as applicable |

Define Severity Levels:

| **Level** | **Description** | **Response Actions** |
| --- | --- | --- |
| Level 1 | Low Impact | Initial assessment and logging |
| Level 2 | Moderate Impact | Incident analysis and containment |
| Level 3 | High Impact | Notification, escalation, and mitigation |
| Level 4 | Critical Impact | Full-scale incident response – perhaps escalate to Business Continuity Plan activation. |

Communication and Notification - internal and external stakeholders:

| **Stakeholder** | **Method of Notification** |
| --- | --- |
| Internal Employees | Email, Intranet |
| Law Enforcement | Phone, Secure Channel |
| Regulatory Agencies | Email, Formal Letter |
| Customers/Clients | Email, Website Notice |
| Media | Spokesperson, Press Release |

Outline of how incident command (IC) will operate:

How IC can be contacted and how often will status updates be provided.

# 4. Incident Response Procedures

4.1 Detection and Analysis:

| **Step #** | **Action** | **Responsible Party** |
| --- | --- | --- |
| 1 | Identify the incident – look for signs of suspicious activity, system outages or unusual data access attempts. | Reporting person |
| 2 | Create an incident log and escalate as needed | Incident Team Lead |
| 3 | Contain the incident – isolate infected system, shutting down internet connection, resetting passwords. | IT Support |
| 4 | Assess the impact – Evaluate the extent of the damage, what data may be compromised, and the potential impact on the organisation’s operations. | IT Support |

4.2 Eradication and Recovery:

| **Step #** | **Action** | **Responsible Party** |
| --- | --- | --- |
| 1 | Preserve evidence for investigation | IT Support/Subject Matter Expert |
| 2 | Eradicate the threat - Remove malware, patch vulnerabilities, or address the root cause of the security incident – Consult relevant Playbook if available. | IT Support/Subject Matter Expert |
| 3 | Recover affected systems - Restore data from backups, rebuild compromised systems, and ensure they are secure before returning them to operation. | IT Support/Subject Matter Expert |

4.3 Risk Assessment and Communications:

| **Step #** | **Action** | **Responsible Party** |
| --- | --- | --- |
| 1 | Assess the risks and consequences of the breach on individuals.* + What are the potential adverse consequences for individuals?
	+ How serious or substantial are these consequences?
	+ How likely are they to happen?
 | Data Protection Person |
| 2 | Report breach to the Data Protection Commission | Data Protection Person |
| 3 | Report breach to the affected individuals (if required) | Data Protection Person |
| 4 | Assess the risks and consequences of the breach on the organisation. | Incident Team Lead/Legal |
| 5 | Keep relevant stakeholders notified. | Communication Lead |
| 6 | Notify Law Enforcement (if required) | Incident Team Lead |

4.4 Post-Incident Activity:

| **Step #** | **Action** | **Responsible Party** |
| --- | --- | --- |
| 1 | Document the incident - Record details of the event, response actions taken, lessons learned, and any remediation steps implemented. | Incident Team Lead |
| 2 | Review and improve - Conduct a post-incident review with your team. Analyse what worked well, identify areas for improvement, and update your incident response plan accordingly. | Incident Team Lead |

# 5. Investigation and Analysis

Conduct a detailed investigation to determine the cause, extent, and impact of the incident.

Preserve evidence for potential legal and regulatory purposes.

Collaborate with law enforcement and other relevant agencies if necessary.

# 6. Documentation and Reporting

Maintain detailed incident logs and documentation.

Prepare incident reports for management, legal, and regulatory purposes.

# 7. Remediation and Recovery

Develop and implement a remediation plan to prevent a recurrence.

Restore affected systems and services to full functionality.

Monitor for any signs of re-infection or reoccurrence.

# 8. Lessons Learned and Post-Incident Review

Conduct a post-incident review with the incident response team.

Identify strengths and weaknesses in the response.

Update the incident response plan based on lessons learned.

# 9. Legal and Regulatory Compliance

Ensure compliance with all legal and regulatory requirements.

Consult with legal counsel as needed.

# 10. Plan Maintenance and Training

Regularly update and test the incident response plan.

Conduct training and drills for the incident response team and employees.

# 11. References and Appendices

Include relevant documentation and reference materials.

A comprehensive contact list should include contact information for all members of the incident response team, key stakeholders, external parties (e.g., law enforcement, legal counsel, regulatory agencies, local authorities, insurers).

Contact details for third-party vendors or service providers who may be involved in incident response activities, such as IT support, forensics experts and incident response consultants.

***Remember that an incident response plan is a living document and should be updated regularly to reflect changes in technology, threats, and organisational structure. Additionally, conducting tabletop exercises and real-world drills can help ensure the effectiveness of your plan.***

# Appendix (a) – Incident Reporting Form:

| **Incident Reporting Form** |  |
| --- | --- |
| **Date and Time of Incident** | [Date] [Time] |
| **Reporting Person's Information** |  |
| * Name:
 | [Reporting Person's Full Name] |
| * Title/Position:
 | [Reporting Person's Title/Position] |
| * Email Address:
 | [Reporting Person's Email Address] |
| * Phone Number:
 | [Reporting Person's Phone Number] |
| **Incident Details** |  |
| * Incident Type:
 |  |
| * Unauthorised Access [ ]
 |  |
| * Malware [ ]
 |  |
| * Data Breach [ ]
 |  |
| * Denial of Service [ ]
 |  |
| * Insider Threat [ ]
 |  |
| * Other (Specify): [ ]
 | [Specify Incident Type] |
| * Description of Incident:
 | [Description] |
| *\* Provide a brief description of the incident, including any relevant details about how it was detected, affected systems, and initial observations.* |  |
| * Location of Incident:
 | [Location] |
| *\* Specify the location or systems where the incident occurred.* |  |
| **Impact Assessment** |  |
| * Severity Level:
 |  |
| * Level 1 (Low Impact) [ ]
 |  |
| * Level 2 (Moderate Impact) [ ]
 |  |
| * Level 3 (High Impact) [ ]
 |  |
| * Level 4 (Critical Impact) [ ]
 |  |
| * Number of Affected Systems/Users:
 | [Number] |
| *\* Specify the approximate number of systems or users impacted by the incident.* |  |
| **Actions Taken** |  |
| * Immediate Response:
 | [Response] |
| *\* Describe the immediate actions taken to address the incident, including containment efforts and isolation of affected systems.* |  |
| * Notification:
 | [Notifications] |
| *\* List any notifications made to internal and external parties, including incident response team members, management, and stakeholders.* |  |
| * Evidence Preservation:
 | [Preservation details] |
| *\* Detail how digital evidence was preserved to support further investigation, if applicable.* |  |
| * Remediation Steps:
 | [Steps] |
| *\* Outline the steps taken or planned to mitigate the incident and prevent a recurrence.* |  |
| **Incident Report Attachments** |  |
| * Screenshots [ ]
 |  |
| * Log Files [ ]
 |  |
| * Network Traffic Captures [ ]
 |  |
| * Other (Specify): [ ]
 | [Specify Attachments] |
| **Incident Reporting Person's Signature:** | [Signature] [Date] |
| **Incident Response Team Initial Assessment:** |  |
| * Assigned Incident ID:
 |  |
| * Assigned Incident Commander:
 |  |
| * Incident Classification:
 |  |
| * Severity Level:
 |  |
| **Additional Comments/Notes:** | [Notes] |
| *\* Provide any additional comments or notes related to the incident.* |  |
| **Confidentiality Notice:** |  |
| *This incident report may contain sensitive and confidential information. Access to and distribution of this report is restricted to authorised personnel involved in incident response and management.* |  |

# Appendix (b) – Incident Log Template:

| **Incident Log** |  |
| --- | --- |
| Incident ID: [Unique Identifier] | Date/Time: [Date and Time] |
| Incident Type: [Type of Incident] | Severity Level: [Severity Level] |
| Person Logging: [Name of person maintaining the log] | Reported By: [Name of Person Reporting] |
| Location of Incident: [Location or Affected Systems] | Status: [Current Status of Incident] |
| **Description of Incident:** |  |
| *\* Briefly describe the incident, including how it was detected, affected systems, and initial observations.* |  |
| **Actions Taken:** |  |
| Date/Time | Action |
| [Timestamp] | [Description of Action] |
| [Timestamp] | [Description of Action] |
| ... (Add additional rows for each action) |  |
| **Notification:** |  |
| Date/Time | Stakeholder |
| [Timestamp] | [Name of Stakeholder] |
| [Timestamp] | [Name of Stakeholder] |
| ... (Add additional rows for each notification) |  |
| **Evidence Preservation:** |  |
| Date/Time | Description of Evidence |
| [Timestamp] | [Description of Evidence] |
| [Timestamp] | [Description of Evidence] |
| ... (Add additional rows for each piece of evidence) |  |

# Appendix (c) – Post Incident Review Template:

| **Post-Incident Review** |  |
| --- | --- |
| Incident ID: [Unique Identifier] | Date of Review: [Date] |
| Incident Type: [Type of Incident] | Review Participants: [List Participants] |
| Incident Severity Level: [Severity Level] | Facilitator: [Name of Facilitator] |
| **Objective of Review:** |  |
| *\* Specify the goal of the post-incident review, e.g., to assess the effectiveness of the incident response process, identify strengths and weaknesses, and make recommendations for improvement.* |  |
| **Review Areas:** |  |
| Area of Review | Findings and Observations |
| **Incident Detection and Reporting** |  |
| * Effectiveness of incident detection methods
 | [Describe findings related to the detection of the incident.] |
| * Timeliness of incident reporting
 | [Describe findings related to the timeliness of reporting.] |
| **Incident Response Actions** |  |
| * Effectiveness of containment and mitigation efforts
 | [Describe findings related to containment and mitigation.] |
| * Coordination and communication among response team members
 | [Describe findings related to team coordination and communication.] |
| **Documentation and Reporting** |  |
| * Accuracy and completeness of incident documentation
 | [Describe findings related to documentation.] |
| * Compliance with legal and regulatory reporting requirements
 | [Describe findings related to legal and regulatory compliance.] |
| **Training and Preparedness** |  |
| * Adequacy of training and readiness of response team members
 | [Describe findings related to training and readiness.] |
| **Additional Findings and Observations** |  |
| *\* List any other findings, observations, or areas of concern identified during the review.* |  |
| **Lessons Learned:** |  |
| *\* Summarise the key lessons learned from the incident and the review process. Highlight both successes and areas for improvement.* |  |
| **Action Items and Follow-Up:** |  |
| *\* List specific action items, responsible parties, and target completion dates for implementing the recommended improvements.* |  |

# Appendix (d) – Playbooks:

**(d)1 Ransomware:**

1. Shut off Internet connection
2. Switch off ALL devices
3. Report incident to An Garda Síochána
4. Contact your insurer - Digital Forensics might be able to determine whether and what data was stolen
5. Assess extent of spread – check for compromise and isolate uninfected devices
6. Check the status of backups

If backups are OK:

* wipe/factory reset all compromised devices
* Restore the data

If backups are corrupt or non-existent:

* Check [www.NoMoreRansom.org](http://www.NoMoreRansom.org) for free decryption tools
* If nothing available and there is no way to recover, pay and 🙏
* Decrypt the data
* Thoroughly check that the data is OK
* Take a backup of the data
* wipe/factory reset all devices
* Restore the data

**(d)2 Email Account Compromise:**

1. Shut off Internet connection
2. Check all mailboxes for forwarding rules – document findings
3. Check all devices for compromise, document findings and isolate uninfected devices
4. Connect IT Admin’s device (if not compromised) to the internet
5. In quick order:
* Change affected email account’s password
* Sign-out all logged in sessions for the email account
* Implement multi-factor authentication on the email account
1. Assess extent of data breach (number and type of impacted emails) – report findings to the Data Protection Person

# Appendix (e) – Incident Response Plan Test Scenarios:

**Scenario 1: Malware Infection**

**Incident Description:** A user reports that their computer is behaving erratically, with a noticeable slowdown in performance. The incident response team suspects a malware infection.

**Scenario 2: Unauthorised Access**

**Incident Description:** An employee reports that they received a suspicious email from an unknown sender, and they suspect an attempted unauthorised access to their email account.

**Scenario 3: Data Breach**

**Incident Description:** A third-party vendor informs your organisation that their database, which contains sensitive customer information, has been breached. They suspect that customer data may have been exposed.

**Scenario 4: Ransomware Attack**

**Incident Description:** Multiple employees report that they are unable to access their files, and a ransom note appears on their screens demanding a cryptocurrency payment to unlock the files. The organisation suspects a ransomware attack.

**Scenario 5: Distributed Denial of Service (DDoS) Attack**

**Incident Description:** The organisation's website experiences a sudden and significant increase in traffic, causing it to become unresponsive. The incident response team suspects a DDoS attack.

**Scenario 6: Insider Threat**

**Incident Description:** A departing employee sends an email to several colleagues containing sensitive organisation information and threats of data leaks. The organisation suspects an insider threat incident.

**Scenario 7: Phishing Attack**

**Incident Description:** Several employees report that they received emails that appear to be from a trusted source but contain suspicious links. The incident response team suspects a phishing attack.

**Scenario 8: Server Compromise**

**Incident Description:** An organisation's server experiences unexpected downtime, and system administrators notice unauthorised access to the server's administrative console. The incident response team suspects a server compromise.

**Scenario 9: Insider Data Theft**

**Incident Description:** An employee who recently resigned is suspected of stealing sensitive organisation data before leaving. The organisation wants to investigate the incident and assess the extent of the data theft.

**Scenario 10: Mobile Device Security Incident**

**Incident Description:** An employee's mobile device, which contains organisation emails and documents, is lost or stolen. The organisation is concerned about potential data exposure and wants to initiate an incident response.

# Appendix (f) – Evidence Preservation Guidelines

**(f)1. Introduction**

Preserving digital evidence is a critical step in the incident response process. Proper preservation ensures the integrity and admissibility of evidence for potential legal and investigative purposes.

**(f)2. Initial Considerations**

Upon detecting an incident, take immediate steps to isolate affected systems or areas to prevent further compromise of evidence.

Do not alter or tamper with the original state of the affected systems or data unless necessary for containment or recovery efforts.

**(f)3. Evidence Identification**

Clearly identify and document the digital evidence to be preserved, including:

* Date and time of evidence collection.
* Location (e.g., server name, file path, network segment).
* Description of the evidence (e.g., log files, system images, network traffic captures).

**(f)4. Chain of Custody**

Establish a chain of custody for each piece of evidence collected. Document the names and roles of individuals who handle the evidence, along with date and time stamps for each transfer or action.

Use standardised chain of custody forms to maintain a clear record of evidence handling.

**(f)5. Evidence Collection**

Follow documented procedures for collecting evidence, which may include:

* Creating a forensic image of affected systems or storage media.
* Collecting relevant log files, configuration data, and volatile memory dumps.
* Capturing network traffic data during the incident.
* Taking screenshots or photographs of visual evidence.
* Labelling and documenting physical evidence, if applicable.

**(f)6. Preservation Media**

Use write-protected and forensically sound media to store evidence. Ensure that the media does not alter the original evidence during storage.

Label preservation media clearly with information such as case identifier, evidence description, and date.

**(f)7. Documentation**

Maintain detailed records of all evidence preservation activities, including:

* Who collected the evidence.
* Date and time of collection.
* Description of the evidence.
* Any actions taken during collection.
* Location of storage media.
* Chain of custody records.

**(f)8. Secure Storage**

Store preserved evidence in a secure and controlled environment, such as a locked evidence room or secure digital storage.

Implement access controls to restrict unauthorised access to evidence.

Protect evidence from physical damage, theft, or tampering.

**(f)9. Periodic Verification**

Periodically verify the integrity of preserved evidence to ensure that it remains unchanged. Use cryptographic hashes or other integrity-checking mechanisms.

Update chain of custody records during verification.

**(f)10. Legal and Regulatory Compliance**

Comply with all legal and regulatory requirements related to evidence preservation, especially when incidents involve potential legal proceedings.

Consult legal counsel for guidance on evidence handling and retention.

**(f)11. Handover Procedures**

Follow documented procedures for handing over evidence to law enforcement or legal authorities, if required. Maintain records of the handover process.

**(f)12. Destruction of Evidence**

Do not destroy preserved evidence without proper authorisation. Document the reason for any evidence destruction and obtain legal consent if necessary.

**(f)13. Training and Documentation**

Ensure that incident response team members are trained on evidence preservation procedures and that the guidelines are documented in the incident response plan.

**(f)14. Continuous Improvement**

Periodically review and update evidence preservation procedures to align with industry best practices and legal requirements.