**Purpose:**

This Incident Response Plan (IRP) outlines how to respond quickly, confidently, and effectively to cybersecurity incidents that could impact our systems, data, operations, or reputation. It forms part of a broader set of Incident Response Program documentation, sitting between the high-level Incident Management Policy and more detailed technical Playbooks and Battlecards.

**Where this fits in your Incident Management Program**: This IRP is the operational middle layer of your wider incident management program:

|  |  |  |
| --- | --- | --- |
| **Crisis Management Plan** | Organisation-wide leadership response to any major disruption | Link |
| **Incident Management Policy** | Strategic authority and scope definition related to all incidents | Link |
| **Cyber Incident Response Plan** | Operational coordination and escalation of cyber incidents | This Document |
| **Playbooks** | Step-by-step guidance for specific cyber incident types | Link |
| **Battlecards** | Fast-access cheat sheets for use during high-pressure, cyber-related scenarios | Link |

**Approval:** This document template is made publicly available by Talanos Cybersecurity for use within your own organisation, where it can be customised, approved and then marked CONFIDENTIAL.

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Author | Version | Changes |
| 1 July 2025 | Talanos Cybersecurity | 1.0 | Initial version – Base Template |
|  |  |  |  |

**Table of Contents**

[1. Scope 3](#_Toc204176041)

[2. Key Definitions 4](#_Toc204176042)

[3. Incident Response Team (IRT) 8](#_Toc204176043)

[4. At-a-Glance Response Flow 11](#_Toc204176044)

[5. Common Incident Categories 12](#_Toc204176045)

[6. Incident Classification and Severity Levels 14](#_Toc204176046)

[7. Incident Response Lifecycle (following the NIST 800-61 framework) 15](#_Toc204176047)

[8. Communications Plan 16](#_Toc204176048)

[9. RACI Snapshot (example) 17](#_Toc204176049)

[10. Incident Log Template (Quick Use) 18](#_Toc204176050)

[11. Appendices 18](#_Toc204176051)

# **Scope**

The protection of <<Insert company name>>’s confidential information is critical. An Information Security Incident can be intentional or unintentional, internal or external, electronic or paper.

This IRP is to be implemented in response to any Information Security Incident.

In addition, this IRP is designed to:

* Meet any notification requirements in the event of an Information Security Incident.
* Protect against threats or hazards to the security or integrity of Confidential Information.
* Conduct a reasonable investigation to determine the likelihood of information that has been or can be misused.
* Appropriately respond to and remediate Information Security Incidents.
* Conduct a post-incident investigation to capture lessons learned.
* Develop or revise written policies and procedures to manage and control these identified risks or vulnerabilities; and
* Adjust the Information Security program to reflect changes in technology, the sensitivity of data stored, and internal or external threats to information security.

# Key Definitions

|  |  |
| --- | --- |
| **Business Sensitive Information or Confidential Information** | Information that is sensitive or proprietary to <<insert company name>> or its customers. This includes, but is not limited to:Personal Information (defined below) that might be collected, used, maintained, or stored at rest, concerning <<insert company name>>’s current, prospective, or former employees, customers, stakeholders, or other third parties in the course of business* Customer or supplier lists
* Financial information, pricing, or contractual information
* Research and development information
* Merger or acquisition information
* Non-public information that if released could potentially cause damage to <<insert company name>>’s operations and business or harm to its reputation
* Trade secrets; and/or
* Other sensitive information.
 |
| **Data breach** | The accidental or unauthorised destruction, loss, alteration, disclosure of, or access to Personal Information (defined below) which may require notification under applicable laws to regulators, and under certain circumstances, individuals. |
| **Event** | An observable occurrence in a system or network. |
| **Information Security Incident** | A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices that may lead to one or more of the following:* Negative impact on the organisation’s reputation
* Inappropriate access or viewing of personal information for either employees or customers
* Access to confidential or private corporate data
* Loss of Intellectual Property
* Loss of funds greater than $XX, XXX

There are a range of adverse events that are Security Incidents, including:* Data breaches,
* Encryption events
* Loss of availability e.g., a distributed denial of service (DDos) attack
* Phishing attacks
* Ransomware
* Business email compromises
* Fraudulent wire transfers, and
* Account takeovers.
 |
| **Personal Information** | Information that relates to or can be used on its own or with other information to identify, contact or locate an individual, or to identify an individual in context.Personal Information includes but is not limited to:* Name
* Home or other physical address
* Email address or other online contact information
* Telephone number
* Social security or similar government identification numbers
* Driver’s license number
* Bank, loan, mortgage, or payment card account number
* Medical information
* Date of birth
 |
| **Personally Identifiable Information (“PII”)** | A subset of Personal Data that is defined by applicable laws and includes certain types of information that is considered particularly sensitive if the data is mishandled or misused, for example:* Social Security Numbers (SSN)
* Driver’s license numbers, state identification numbers, tax identification numbers, military identification numbers, or other unique identification numbers issued on a government document commonly used to verify the identity of a specific individual
* Passport numbers
* Medical or health-related information, genetic information, and biometric data
* Financial account information
* Personal account credentials, including passwords and security questions and answer information.
 |
| **Ransomware** | A form of malware that encrypts a victim’s files or data. The attacker then demands a ransom from the victim in exchange for restoring access to the files, data, systems, etc. |
| **Threat Actor** | An individual or group posing a threat or responsible for a cyber attack. |

# **Incident Response Team (IRT)**

The <<insert company name>> Incident Response Team (IRT) has been established to provide a quick, effective and orderly response to an Information Security Incident.

The IRT shall consist of identified individuals with appropriate skills and specific knowledge necessary to successfully handle and investigate incidents and strategically guide the team.

The goals of the IRT are:

* Identifying, responding to, analysing, and investigating Information Security Incidents.
* Minimising the negative impact of incidents on the organisation and its business.
* Performing root cause analysis and proposing solutions for improvement.
* Collecting and preserving actionable evidence related to the incident for submission to regulatory authorities if needed.

The IRT shall be led by the Incident Manager.

Membership of the IRT will be reviewed annually by the IRT Leader and updated as needed.

|  |  |  |  |
| --- | --- | --- | --- |
| **Role** | **Name** | **Responsibility** | **Contact Info** |
| Incident Manager | [Name] | Coordinates the overall response | [Phone/Email] |
| IT Lead | [Name] | Containment & eradication | [Phone/Email] |
| Comms Lead | [Name] | Internal/external communication | [Phone/Email] |
| Legal/Compliance | [Name] | Regulatory response & reporting | [Phone/Email] |
| HR | [Name] | Staff-related issues | [Phone/Email] |

**Escalation Guidelines**

The IRT is responsible for assessing all identified incidents and determining whether escalation is required. The following escalation process applies:

**1. Initial Assessment**

All potential security incidents must be reported to the IRT without delay.

The IRT will perform an initial triage to determine if the event qualifies as an Information Security Incident under this IRP.

**2. Escalation Criteria**

An incident should be escalated if any of the following apply:

* Involves sensitive or regulated data (e.g., PII, PCI, health data)
* Impacts business-critical systems or services
* Shows signs of external threat actor involvement
* Triggers legal, contractual, or regulatory obligations
* Requires forensic investigation or legal oversight
* May result in reputational damage or public disclosure

**3. Escalation Tiers**

|  |  |  |  |
| --- | --- | --- | --- |
| **Tier** | **Trigger** | **Escalated To** | **Examples** |
| **Tier 1** | Low severity (isolated, no data loss) | IRT Lead | Malware flagged on endpoint, no spread. |
| **Tier 2** | Medium severity (business disruption or internal data) | Managed SOC provider, IT Director | Internal system compromise, employee data accessed. |
| **Tier 3** | High severity (regulated data or major outage) | CISO, Legal Counsel, External Forensics | Ransomware with potential exfiltration |
| **Tier 4** | Critical (significant reputational/regulatory impact) | Exec team, Comms, Legal, DPO | Confirmed data breach, public disclosure required |

**4. Escalation Workflow**

Once escalation is triggered:

* The IRT Lead informs appropriate internal and external stakeholders (e.g., SOC, legal, HR, communications).
* The incident is assigned a severity level based on predefined criteria (see Incident Classification and Severity Levels).
* Responsibilities are reassessed, and additional workstreams (e.g., Investigation, Communications) are activated as needed.

If external legal counsel or forensic consultants are required, they are to be engaged immediately.

**5. Ongoing Review**

Escalation status should be reassessed as new information becomes available. An incident may be de-escalated or escalated further based on evolving severity, scope, or impact.

###

#  **At-a-Glance Response Flow**



Image courtesy of the NCSC (<https://www.ncsc.gov.uk/collection/incident-management/cyber-incident-response-processes> )

1. **Detection & Triage** – Confirm an incident from alerts or reports
2. **Assessment / Analysis** – Assign severity, notify stakeholders
3. **Containment / Mitigation** – Stop spread and damage
4. **Remediation / Eradication** – Remove the threat
5. **Recovery** – Restore services
6. **Review** – Capture lessons learned

# **Common Incident Categories**

* **Unauthorised access**
	+ Access to systems, applications, or data by individuals who do not have the necessary permissions. This includes external attackers breaching accounts, or internal users exceeding their access rights (intentionally or accidentally).
* **Malware / ransomware**
* Malicious software designed to disrupt, damage, or gain unauthorized access to systems.
	+ - **Malware** includes viruses, worms, spyware, and trojans.
		- **Ransomware** specifically encrypts files or systems and demands payment for restoration.
* **Insider threats**
	+ Security risks originating from within the organisation - such as employees, contractors, or partners - who misuse access to harm the company, either maliciously (e.g. data theft) or negligently (e.g. poor security practices).
* **Data breaches**
	+ Incidents where sensitive, confidential, or protected data is accessed, disclosed, or stolen without authorisation. This can result from cyberattacks, human error, or physical loss of data storage devices.
* **Lost/stolen devices**
	+ When company laptops, phones, USB drives, or other equipment containing or providing access to sensitive data are lost or stolen. These incidents can lead to data exposure if the devices are not properly encrypted or secured.
* **Denial-of-Service (DoS) attacks**
	+ An attempt to make a system, service, or network unavailable to users, typically by overwhelming it with traffic. This includes:
		- **DoS** (single source)
		- **DDoS** (Distributed Denial-of-Service: multiple sources)

# **Incident Classification and Severity Levels**

|  |  |  |  |
| --- | --- | --- | --- |
| **Level** | **Description** | **Impact Criteria** | **Examples** |
| **Low** | - No impact on business operations.- Incident is contained and poses no ongoing risk. | - No data accessed or lost- No system downtime- Handled by user or Helpdesk | - Blocked phishing email- Unusual login attempt flagged and blocked- Misdelivery of non-sensitive internal email |
| **Medium** | - Localised impact with minor disruption.- Limited to a single user, endpoint, or low-priority system. | - Non-critical system affected- Temporary loss of access or performance- No sensitive data involved | - Malware detected and removed from a laptop- Misuse of VPN credentials- Personal data emailed internally |
| **High** | - Significant disruption or exposure.- Affects critical systems, sensitive data, or multiple users. | - Disruption to business functions- Involves confidential or personal data- Potential financial or reputational damage | - Ransomware on a departmental server- Insider copying sensitive files- Compromised credentials used to access systems |
| **Critical** | - Severe or widespread impact.- Regulatory breach, high-value data exposure, or risk to public trust. | - Legal or regulatory implications- Large-scale customer impact- Extended downtime of critical systems | - Breach of customer data- Attack on core infrastructure (e.g. ERP, CRM)- Widespread ransomware outbreak |

# Incident Response Lifecycle (following the NIST 800-61 framework)

#### Preparation

* Conduct training & tabletop exercises
* Maintain asset inventory and backups
* Define response roles and escalation matrix

#### Detection & Analysis

* Monitor SIEM/EDR alerts, user reports
* Validate incident & gather evidence
* Begin incident log entry

#### Containment, Eradication & Recovery

* Isolate affected systems, reset credentials
* Remove malware and remediate vulnerabilities
* Restore from backups, test before reintroducing

#### Post-Incident Activity

* Run a review meeting (see review template)
* Document lessons learned
* Update playbooks, tools, and training

# Communications Plan

Who communicates, when, and to whom?

* Notify internal teams and exec sponsors
* Engage legal / compliance for regulatory reports
* Provide external comms for media / customers

Refer to approved templates (see appendices) or to a higher-level incident management document if required.

# RACI Snapshot (example)

**RACI** is a responsibility assignment matrix used to clarify roles during incident response and other workflows. It defines who is:

* **Responsible** – The person(s) doing the work to resolve the task or incident.
* **Accountable** – The individual ultimately answerable for the outcome; they approve decisions and ensure completion.
* **Consulted** – Stakeholders or subject matter experts whose input is needed before decisions or actions.
* **Informed** – Individuals who must be kept updated on progress or decisions but are not directly involved in the work.

| **Phase** | **Incident Manager** | **IT Lead** | **Comms** | **Legal** | **Managed SOC** |
| --- | --- | --- | --- | --- | --- |
| Detection | A | R | C | I | R |
| Containment | A | R | I | C | R |
| Communications | C | I | A | C | I |
| Recovery | A | R | I | I | R |
| Post-Incident | A | R | C | C | R |

# **Incident Log Template (Quick Use)**

| **Date / Time** | **Incident ID** | **Description** | **Severity** | **Actions Taken** | **Outcome** | **Owner** |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

# **Appendices**

* Internal/external contact list
* Scenario playbooks (e.g. ransomware, phishing)
* Battlecard examples
* Breach notification templates
* Post-incident review form
* Compliance mapping (ISO, GDPR, NIST)
* Tabletop exercise guide