INCIDENT RESPONSE POLICY

*Revision: r1.0*

*Effective Date: ddmmyyyy*

*Classification: INTERNAL*

**INTERNAL INFORMATION**

This is a proprietary document and is the property of XXXX.; it contains information that is proprietary, or otherwise restricted from disclosure. If you are not an authorised recipient, please return this document to the above-named owner(s). Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of XXXX..

Table of Contents

1. Introduction 3

1.1 Document Definition 3

1.2 Objective 3

1.3 Scope 3

1.3.1 Applicability to Employees 3

1.3.1 Applicability to External Parties 3

1.3.2 Applicability to Assets 3

1.4 Related Documents / References 3

2. Policy Statements 4

2.1 Incident Response Plan 4

2.2 Incident Response Plan Responsibility 4

2.3 Incident Response Process Ownership 4

2.4 Business Unit Participation 4

2.5 Employee Responsibility 4

2.6 Incident Monitoring and Response Availability 4

2.7 Incident Response Procedures 4

2.8 Rapid Response 5

2.9 Documentation and Reporting 5

2.10 Qualified Personnel 5

2.11 Evidence Collection 5

2.12 Information Integrity 5

2.13 Information & Evidence Release 5

2.14 Contact with External Authorities 5

2.15 Lessons Learned / Evolving Threat Landscape 5

2.16 Incident Response Review 6

2.17 Protection of Log Files 6

3. Policy Compliance & Enforcement 7

3.1 Compliance Measures 7

3.2 Enforcement 8

4. Exception Process / Glossary 9

4.1 Exception Process 9

4.2 Glossary / Acronyms 9

5. Document Management 10

5.1 Document Revision Log 10

5.2 Document Ownership 10

5.3 Document Coordinator 10

5.4 Document Approvers 10

5.5 Document Distribution 10

# Introduction

## Document Definition

This document is a Policy.

For a full description of document types, see XXXX-POL-ALL-001 *- Information Security Policy Framework*.

## Objective

The objective of this policy is to provide information security requirements for incident response to unplanned information System Asset events, including network intrusions or denial of service, computer virus outbreaks, and other outages that negatively impact the confidentiality, integrity, and/or availability of XXXX (XXXX) systems, applications, and/or information assets.

## Scope

### Applicability to Employees

XXXX refers to XXXX as well as its majority-owned subsidiaries and joint ventures (if applicable). This Policy applies to all employees, officers, members of Board of Directors, and all consultants, and contractors.

### Applicability to External Parties

Relevant Policy statements will apply to any external party and be included in contractual obligations on a case-by-case basis.

### Applicability to Assets

This Policy applies to all information assets globally owned by XXXX, or where XXXX has custodial responsibilities.

## Related Documents / References

* *XXXX-POL-ALL-001 - Information Security Policy Framework*
* *XXXX-POL-ALL-008 - Business Continuity Management Policy*
* *XXXX-POL-ALL-013 - Disaster Recovery Policy*
* *XXXX-PRC-ALL-006 - Incident Response Procedure(s)*
* *XXXX-PRC-ALL-015 - Vulnerability Management Procedure*

# Policy Statements

## Incident Response Plan

An Incident Response and Escalation Plan (IRP) is developed as part of *XXXX-PRC-ALL-006 - Incident Response Procedure(s)*. The IRP will be a complete, documented reference of the XXXX [Incident Response Team (IRT) process.

## Incident Response Plan Responsibility

The Head of IT/Information Security Unit shall be responsible for creating and distributing the IRP.

## Incident Response Process Ownership

A designated responsible authority must be assigned to oversee the Incident Response process, ensuring that each incident is appropriately managed.

## Business Unit Participation

Business units must designate an individual to participate on an incident response team and provide subject matter input to aid the incident response process.

## Employee Responsibility

All employees must report immediately any suspected computer security event/incident following their local notification procedures.

All employees must report immediately any suspected data breach to IT Helpdesk

## Incident Monitoring and Response Availability

Both monitoring and alert processes and the XXXX Incident Response Team (IRT) must be available on a 24 X 7 X 365 basis. Incident coverage must include, but not be limited to:

* Evidence of unauthorised activity.
* Detection of unauthorised wireless access points.
* Critical IDS / IPS alerts.
* Reports of unauthorised critical system or application file changes.

## Incident Response Procedures

Information security incident response procedures must include, but are not limited to, the following:

* Specific roles and responsibilities.
* Key contact information (call trees), including key vendor contacts.
* High-level guidelines for investigating, documenting and reporting security incidents.
* Alerts from security monitoring systems (IDS/IPS, firewalls, logging mechanisms etc.).

## Rapid Response

The designated responsible authority must respond rapidly to all security incidents, liaising and coordinating with colleagues to gather information and offer advice. These activities include, but are not limited to:

* Evaluating the current state of the system, the extent of penetration or infection, the type of data at risk and the source or target of the attack.
* Isolating and containing the threat in order to disengage the threat and track and identify the attacker.
* Overseeing recovery and restoration.
* Beginning system remediation and identifying issues that may have contributed to the security breach.

## Documentation and Reporting

Evidence relating to a suspected Information Security incident must be formally recorded, processed, and reported to designated XXXX IT representatives. The IRT will ensure that the evidence is retained to support further investigations or legal pursuit.

## Qualified Personnel

Information Security incidents must be properly investigated by suitably trained and qualified personnel. Training will be provided on an as-needed basis.

## Evidence Collection

Evidence related to a security event must be logged, stored in a central location, and follow all best practices related to chain of custody.

## Information Integrity

During an investigation of Information Security incidents, dual control and segregation of duties as they relate to the nature of the investigation must be enforced to protect the integrity of information and data.

## Information & Evidence Release

Information relating to an Information Security incident must only be released (internally and externally) by authorised XXXX personnel.

## Contact with External Authorities

All external reporting of Information Security Incidents required by law or regulatory compliance must be performed by both the XXXX Information Security Committee and the Legal Department.

## Lessons Learned / Evolving Threat Landscape

The Incident Response Procedure must be updated in light of lessons learned during each iteration of the Vulnerability Management process cycle, and considering changes to the evolving threat landscape per *XXXX-PRC-ALL-014 - Vulnerability Management Procedure*.

## Incident Response Review

Relevant systems incident response plan(s) as detailed in the XXXX-*PRC-ALL-006 - Incident Response Procedure(s)* will be tested at a minimum annually, and after any significant changes to business or technical processes.

## Protection of Log Files

Log files and other related monitoring output from information system assets must be protected from unauthorised changes or access.

# Policy Compliance & Enforcement

## Compliance Measures

If applicable, compliance with the above Policy can be measured by the following criteria. Example evidence will vary depending on any supporting guidelines implemented to support this Policy. The following list is not exhaustive, and all example evidence types may not be required to validate compliance.

Evidence of compliance can be presented in hard copy or electronic format.

|  |  |
| --- | --- |
| **Criteria** | **Example Evidence** |
| Evidence that incident response procedures have been assigned to appropriate personnel (ownership and participation) | * Interviews with key personnel * Job descriptions * Incident response procedures * Training / awareness materials (Intranet site, etc.) |
| For a selection of incident response procedures, evidence that the procedures include:   * Specific roles and responsibilities * Key contact information (calling trees), including key vendor contacts   High-level guidelines for investigating, documenting and reporting security incidents | * Incident response procedures |
| For a selection of incident responses, evidence that the authority responded with at least the following actions:   * Evaluating the current state of the system, the extent of penetration or infection, the type of data at risk and the source or target of the attack * Isolating and containing the threat in order to disengage the threat and track and identify the attacker * Overseeing recovery and restoration * Enforcing additional controls   Beginning system remediation and identifying issues that may have contributed to the security breach | * Incident response report / results * Completed checklists * Email communication * Automated trouble-ticketing system notes * Root-cause analysis documentation |
| For a selection of incident responses, evidence that the relevant details were recorded, processed, and reported to management | * Incident response report / results * Completed checklists * Email communication * Automated trouble-ticketing system notes * Root-cause analysis documentation * Incident response executive summary |
| For a selection of incident response information released internally and externally, evidence that the release of information was authorised and reviewed by legal or corporate communications | * Interviews with key personnel * Incident response executive summary * Press releases |

## Enforcement

All staff of XXXX must comply with all Information Security Policies. Failure to comply with these policies may result in disciplinary action in accordance with the current XXXX Human Resources policy. Disciplinary actions may include, but are not limited to:

* verbal and/or written warnings;
* instant dismissal; and
* actions by judicial and regulatory authorities.

# Exception Process / Glossary

## Exception Process

Non-compliance with the Policy statements described in this document must be reviewed and approved in accordance with the Exception Process defined in XXXX-POL-ALL-001 *- Information Security Policy Framework*.

## Glossary / Acronyms

|  |  |
| --- | --- |
| CSIRT | Computer Security Incident Response Team |
| IDS | Intrusion Detection Systems |
| IPS | Intrusion Protection Systems |
| Security event | An information *security event* is a system, service, or network state, condition, or occurrence that indicates that information security may  have been breached or compromised or that a security policy may  have been violated or a control may have failed. |
| Security incident | An information *security incident* is made up of one or more unwanted or unexpected information security events that trigger an investigation to determine if there has been a compromise in the security of information or impairment of business operations. |
| Data Breach | A *data breach* is an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorised to do so. |

# Document Management

## Document Revision Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Editor** | **Revision #** | **Description of Change** |
|  |  |  |  |
|  |  |  |  |

## Document Ownership

This Policy is owned by the YYYY.

## Document Coordinator

This Policy is coordinated by the YYYY.

## Document Approvers

|  |  |  |
| --- | --- | --- |
| **Approver Name** | **Signature** | **Date** |
|  |  |  |
|  |  |  |

## Document Distribution

The Document Owner controls distribution of this document. The distribution is as follows:

* All Staff