COMPANY LOGO

**Incident Response Plan**

**Updated:**

Company is hereinafter referred to as "**Company**” or “**the Company**."

# Overview

A security incident can come in many forms: a malicious attacker gaining access to the network, a virus or other malware infecting computers, or even a stolen laptop containing confidential data. A well-thought-out Incident Response Plan is critical to successful recovery from an incident. This Incident Response Plan (“**Plan**”) covers all incidents that may affect the security and integrity of the Company's information assets, and outlines steps to take in the event of such an incident.

# Incident Response Plan

This Incident Response Plan guides the Company during a cyber Security Event, Incident or Breach. This Plan guides the response in a systematic manner to security incidents, events and breaches and is designed to:

1. address disruption of critical information systems;
2. address loss or theft of sensitive or critical information; and
3. remediate and recover from security events.

## 2.1 Definitions

**Security Event** – Potential impact to key business functions, systems, or sensitive personal information. Examples may include a lost unencrypted laptop believed to contain employee or member data, potential unauthorized access to elevated network administrator credentials, or unexplained malfunctions of security appliances. While it may seem initially significant, further investigation determines that it is not an incident, and so the event will be managed by the Information Security team according to documented procedures. If the initial information shows a low severity and low likelihood of potential impact on core business functions, systems, or sensitive personal information, an incident will not be declared, and the event will be managed according to procedures. Examples may include attempted systematic website or network perimeter probes, commodity malware infections, or unexplained system malfunctions of user workstations or other non-core production devices.

**Security Incident** – High likelihood of or confirmed unauthorized access to critical systems or access or acquisition of sensitive information. Examples include reports from third parties of confirmed theft of employee Social Security numbers, cyber-extortion demands, or unexplained outbound data flow.

**Security Breach** – Unlawful and unauthorized acquisition and/or access of confidential information that compromises the security, confidentiality, or integrity of the information.

## 2.2 Incident Response Team and Support Roles

The key players in responding to a situation are identified as follows:

| **Title** | **Role & Responsibilities** |
| --- | --- |
| **Incident Response Team (Core)** | The core members of the Incident Response Team are responsible for determining the nature of the event and determining if an incident has occurred. This team will be responsible for the initial risk assessment, declaration of an incident, and escalating to the full Incident Response Team. Members of the Incident Response Team are listed in [Appendix A](#_Appendix_A_–). |
| **Legal** | The role of Legal is to provide advice as needed during the incident. This can include ensuring the protection of privilege, the legal usability of evidence collected, and handling any potential liability issues. |
| **Incident Response Team (Secondary)** | The Incident Response Team is responsible for assessing the extent and potential damage of the incident, handling communications about the incident, and identifying next steps. |
| **Executive Management** | The role of Executive Management is to facilitate decision making during an incident. |
| **Marketing & Communications** | The Marketing & Communications team, led by the VP, Marketing, can best advise how to communicate information to the general public. |
| **Information Security Team** | The Information Security Team is responsible for assisting in the investigative tasks including preservation and analysis of collected evidence at direction of the CPO & IT Director. |

This Incident Response Plan describes who is involved in each incident phase along with the associated procedures.

## 2.3 Incident Response Procedures

Cyber incident response involves the following elements.

### First Response

Documented procedures for reporting and verifying a suspected incident are critical. Any end user who observes something suspicious should have a clear understanding of who to notify. First responders must engage in evidence preservation procedures to ensure documentation and appropriate handling of any initial investigation steps.

### Incident Declaration

The IT Director will meet the core members of the Incident Response Team as deemed necessary and decide what type of Security Incident or Breach has occurred.

### Notification and Escalation

Once an incident or breach has been declared, certain communications need to occur:

**Internal Communications.**

**Third Party Communications**.

**External Communications**.

Once an incident or breach is declared, the Incident Response Team will need to determine what third party resources may be needed to manage the security incident. Considerations may include:

**Computer Forensics Firm**

**External Law Firm/Breach Counsel**

**Cybersecurity Insurance**

**Law Enforcement**

**Crisis Communications Firm**

### Preservation of Evidence

Evidence preservation is critical. This can include servers, workstations, mobile devices, and log files. Upon declaration of an incident or breach, the team needs to quickly locate and preserve any devices that are suspected of involvement.

### Analysis of Evidence

Once preserved, evidence should be analyzed by forensic team. Depending on the nature of the incident, this can include analysis of log files and system output, and review of interview notes.

### Implementation of Containment Strategies

The containment strategy should be identified and executed by the appropriate security resource or third party forensic firm. These activities can include implementing technical measures such as end point threat monitoring, removing affected devices from the network, adding firewalls, changing firewall settings, revoking user accounts, and removing unnecessary access.

### Eradication of Attack Tools

During the incident, all attacker hooks and tools must be identified and removed from the Company network.

### Recovery: Lessons Learned and Mitigating Controls and Processes

The final stage of the incident is to conduct an after-action report.

## 2.4 Planning, Testing & Training

The Company will develop a process for continual review and testing of the plan. Reviews shall occur at least annually or following major changes to some material part of the incident response process.

# Process Communication Flow

During an investigation, roles & responsibilities must be clearly understood.

Legal will manage communications with Law Enforcement. Additionally, Legal is responsible for providing a legal opinion as to whether or not notification is necessary and providing input on the communications sent to the notification population.

Depending on the nature of the incident, other third parties may be necessary: Computer Forensics, Vendors, etc.

The Marketing & Communications team is responsible for communicating information to the general public. However, this will also be done with the review of Counsel. A Crisis Communications firm may be necessary for notification purposes. A Public Communications Procedure should outline the situations in which information should be released to the public.

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Revision | Date | Name | Description |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Appendix A – Incident Response Team Contact Information

Current contact information for all Incident Response Team members and third parties is documented and updated on a periodic basis to ensure it is accurate. This list includes not just Company employees, but any key service providers who may need to be contacted in the event of an incident. After hours contact information is also included.

This Key Personnel Contact Information document is maintained separately and is provided as a reference with the Incident Response Policy.

## Internal Contacts

| **Name, Title** | **Contact Option** | **Contact Number** |
| --- | --- | --- |
|  | Phone |  |
| Email |  |
| Mobile |  |
| Other |  |
|  | Phone |  |
| Email |  |
| Mobile |  |
| Other |  |
|  | Phone |  |
| Email |  |
| Mobile |  |
| Other |  |
|  | Phone |  |
| Email |  |
| Mobile |  |
| Other |  |
|  | Phone |  |
| Email |  |
| Mobile |  |
| Other |  |

## External Contacts

| **Name, Title** | **Contact Option** | **Contact Number** |
| --- | --- | --- |
| **Site Security** | | |
|  |  |  |
|  |  |  |
| **Landlord** | | |
|  |  |  |
|  |  |  |
| **Property Management, Building Maintenance** | | |
|  |  |  |
|  |  |  |
| **Insurance** | | |
|  | Phone |  |
|  | Email |  |
| **Legal** | | |
|  |  |  |
|  |  |
| **Credit Agencies** | | |
| Experian |  | 1-888-397-3742 |
| Equifax |  | 1-800-525-6285 |
| TransUnion |  | 1-800-680-7289 |
| **Law Enforcement** | | |
|  |  |  |
|  |  |  |
| **Media/Crisis Communications** | | |
|  |  |  |
| **Forensic IT Consultant** | | |
|  |  |  |