Incident Response Plan

Purpose

ORG maintains an Incident Response Plan to safeguard our digital assets, protect sensitive information, and maintain operational continuity in the face of potential security threats. This plan serves several critical purposes:

1. Rapid Threat Mitigation: It enables us to quickly identify, contain, and neutralize security incidents, minimizing potential damage and data loss.
2. Operational Resilience: By having predetermined procedures in place, we can swiftly restore normal operations, reducing downtime and associated costs.
3. Regulatory Compliance: The plan helps us meet legal and industry-specific requirements for incident reporting and management.
4. Coordinated Action: The plan defines roles, responsibilities, and communication channels, ensuring a cohesive response across our ORG.

By maintaining and regularly updating this Incident Response Plan, ORG strengthens its overall security posture, protects its reputation, and ensures its ability to deliver uninterrupted service to our constituents and stakeholders.

Scope

This Incident Response Plan policy is designed specifically for and applies to all members of the Incident Response Team. It outlines comprehensive guidelines for team members, detailing the process for implementing a response to potential security breaches. To ensure its effectiveness, the policy will be made readily accessible to all Incident Response Team members at all times.

While the primary focus of this policy is on the Incident Response Team, it's important to note that all staff at [ORG] play a role in maintaining security. As such, all employees will receive guidance on reporting suspected incidents through the Technology Acceptable Use Policy, which they will be required to review and sign. This approach ensures a cohesive and ORG-wide commitment to incident response and security awareness.

Background

The primary objective of [ORG]'s Information Security Program is to detect and address security vulnerabilities proactively, thereby preventing incidents and breaches. [ORG] places a high priority on safeguarding its network and data against unauthorized actions that could compromise its operations and mission.

Recognizing that incidents may still occur despite preventive measures, [ORG] is committed to a swift and effective response process. This process encompasses detection, containment, investigation, and resolution, followed by comprehensive communication with all relevant stakeholders.

All users within [ORG] are required to report any observed or suspected security issues promptly, as detailed in this document. To enhance the detection of vulnerabilities and incidents, [ORG] utilizes automated tools for scanning and monitoring its systems and networks.

Upon identifying a vulnerability or incident, [ORG] will take appropriate actions based on the assigned severity level. In the event of a confirmed breach, [ORG] will execute a predefined procedure to address and resolve the situation, including notifying affected individuals and partners as necessary.

This Incident Response Plan outlines the framework for managing these processes, ensuring [ORG] can respond effectively to security threats while minimizing potential impacts on its operations and stakeholders.

This document also clarifies terms and definitions relevant to [ORG]'s incident response efforts.

Within this document, the following definitions apply:

Information Security Vulnerability:

A vulnerability in an information system, information system security procedures, or administrative controls that could be exploited to gain unauthorized access to information or to disrupt critical processing.

Information Security Incident:

A suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of information; interference with information technology operations; or significant violation of information security policy.

Roles and Responsibilities

Effective incident response at [ORG] depends on clear role definition and coordinated teamwork. Our incident response framework encompasses key roles covering all aspects of incident management, from detection to post-incident review. The following table outlines these roles and their responsibilities, serving as a guide for all team members. Understanding these roles is crucial for efficient incident handling and maintaining our ORG's security posture.

The following individuals will be responsible for the roles as described below.

Role	Responsibilities
Incident Response Team Lead	● Oversees the incident response process from detection to resolution ● Coordinates communication between internal teams and external parties ● Makes critical decisions during incident response.
Technical Lead	● Leads the initial assessment of the incident to determine its scope and impact. ● Implements security measures to contain and mitigate the incident ● Advises on the technical aspects of the response and recovery efforts.
Data Governance Lead	● Assists in evaluating the impact on data due to security incidents. ● Ensures adherence to data privacy laws during incident response.
Legal	● Provides guidance on legal and regulatory obligations following an incident. ● Assists with communication strategies to ensure compliance ● Advises on potential legal ramifications and actions.
Communications	● Prepares internal and external communications regarding the incident. ● Coordinates with stakeholders to provide updates and resolve

	concerns.
Human Resources	● Addresses personnel issues related to the incident. ● Manages support services for affected individuals.
All Employees and Contractors	● Report suspected security incidents or vulnerabilities through established channels. ● Comply with security policies and procedures. ● Participate in awareness training and incident response exercises as required.

Policy

Incident Reporting

- All users, including employees and contractors, are required to report any signs of system vulnerabilities, security incidents, or events that may indicate a potential security breach. Such reports should be made to the Technical Lead as promptly as possible, and no later than 24 hours from discovery.
- Incident reports should be submitted via email, detailing the nature of the incident, observations, and any other relevant information that can aid in the incident response process.

Training and Compliance

- Users will receive training on the procedures for reporting security incidents and vulnerabilities, along with their responsibilities to ensure timely reporting. This training will be conducted regularly to ensure all users are aware of the process and the importance of their role in safeguarding the ORG’s information assets.
- Failure to report information security incidents is considered a breach of security policy and will result in disciplinary action, managed by the Human Resources Department. The severity of the action will correspond to the nature and impact of the unreported incident.

Preservation of Evidence

- In the event of a security incident, all related information and artifacts (including files, logs, and screenshots) must be preserved securely. This evidence is critical for analyzing the incident and may be required for legal proceedings or crime investigation.

Response and Management

- All information security incidents, once reported, will be addressed following the detailed incident management procedures outlined in subsequent sections of this document. These procedures ensure a structured and effective approach to incident response, from initial analysis to resolution and post-incident review.

Periodic Evaluation

It is important to note that the processes surrounding security incident response should be periodically reviewed and evaluated for effectiveness. This also involves appropriate training of resources expected to respond to security incidents, as well as the training of the general population regarding [ORG]'s expectation for them, relative to security responsibilities. The incident response plan is tested annually.

Procedure for Establishing Incident Response System

On-Call Schedule and Information Security Manager Assignment:

- Develop an on-call schedule that ensures continuous coverage by an Information Security Manager (ISM) to manage the incident response procedures across all availability windows.
- Assign an Technical Lead for each shift or window, responsible for overseeing the incident response during their designated times.

Notification Channel:

- Establish a dedicated notification channel for alerting the on-call Technical Lead about potential security incidents promptly.
- Maintain a secure and easily accessible company resource containing up-to-date contact information for the on-call ISM, ensuring that any member of the ORG can quickly reach them in case of an incident.

Management Sponsor Assignment:

- Assign management sponsors from key departments including, Legal, HR, Marketing, and Information Technology to support and provide resources for the incident response efforts.
- These sponsors will play a pivotal role in ensuring cross-departmental coordination and support for the incident response process.

Distribution of Incident Response Procedures:

  - Distribute the "Procedure for Executing Incident Response" documentation to all staff members, ensuring they are informed about the steps to follow in case of a security incident.
  - Guarantee that the most current version of the incident response procedures is always accessible to all employees in a dedicated company resource, such as an intranet or secure document repository.

Training Requirement:

  - Mandate that all staff members included in the incident response team complete a tabletop exercise to test the incident response plan at least once per year to ensure they are familiar with their roles and responsibilities in the event of an incident.
  - This training should include practical exercises and simulations to prepare staff for a variety of potential security incident scenarios.

Reporting Incidents

Staff must report any of the following situations as they may indicate a security event requiring immediate attention:

- Ineffective Security Controls: Any signs that security measures are not performing as intended.
- Compromise of Information: Incidents involving the loss of integrity, confidentiality, or availability of information.
- Human Errors: Mistakes made by staff or users that could impact security or data protection.
- Policy or Guideline Violations: Any actions or activities that deviate from established ORGal policies or guidelines.
- Physical Security Breaches: Unauthorized access or breaches of physical security barriers or protocols.
- Uncontrolled System Changes: Modifications to systems or configurations that were not approved or documented.
- Software or Hardware Malfunctions: Failures or malfunctions in software or hardware that could jeopardize system security.
- Access Violations: Unauthorized access attempts or breaches in access control mechanisms.

- Anomalous System Behavior: Unusual system activity that could indicate a security attack or an actual security breach.

Procedure For Executing Incident Response:

1. When an information security incident is identified or detected, users must notify their immediate manager and the Technical Lead within 4 hours. The following information must be included as part of the notification:
    1. Description of the incident
    2. Date, time, and location of the incident
    3. Person who discovered the incident
    4. How the incident was discovered
    5. Known evidence of the incident
    6. Affected system(s)
2. Within 4 hours of the incident being reported, the Technical Lead shall conduct a preliminary investigation and risk assessment to review and confirm the details of the incident. If the incident is confirmed, the Technical Lead must assess the impact to [ORG] and with the Incident Response Team Lead, assign a severity level, which will determine the level of remediation effort required:
    1. **High**: the incident is potentially catastrophic to [ORG] and/or disrupts [ORG]'s day-to-day operations; a violation of legal, regulatory or contractual requirements is likely.
    2. **Medium**: the incident will cause harm to one or more business units within [ORG] and/or will cause delays to a business unit's activities.
    3. **Low**: the incident is a clear violation of ORGal security policy, but will not substantively impact the business.
    4. **Non-incident:** The reported event is determined not to be an incident.
3. The Technical Lead, in consultation with management sponsors, shall determine appropriate incident response activities in order to contain and resolve incidents.
4. The Technical Lead must take all necessary steps to preserve forensic evidence (e.g. log information, files, images) for further investigation to determine if any malicious activity has taken place. All such information must be preserved and provided to law enforcement if the incident is determined to be malicious.
5. The Technical Lead must take all necessary steps to resolve the incident and recover information systems, data, and connectivity. All technical steps taken during an incident must be documented in [ORG]'s incident log, and must contain the following:

   1. Description of the incident
   2. Incident severity level
   3. Root cause (e.g. source address, website malware, vulnerability)
   4. Evidence
   5. Mitigations applied (e.g. patch, re-image)
   6. Status (open, closed, archived)
   7. Disclosures (parties to which the details of this incident were disclosed to, such as customers, vendors, law enforcement, etc.)

6. After an incident has been resolved, the Technical Lead must conduct a post-mortem that includes root cause analysis and documentation of any lessons learned.
7. Depending on the severity of the incident, the Chief Executive Officer (CEO) may elect to contact external authorities, including but not limited to law enforcement, private investigation firms, and government ORGs as part of the response to the incident.
8. The Technical Lead must notify all users of the incident, conduct additional training if necessary, and present any lessons learned to prevent future occurrences. Where necessary, the HR Manager must take disciplinary action if a user’s activity is deemed as malicious.

Appendix A: Security Incident Report Template

Incident Response Report

Incident Name

Date

Report created by	*NAME*
Peer-reviewed by	*NAME*
Management-reviewed by	*NAME*

Steps:

1. Make a copy of this Template (please do not EDIT this template)
2. Complete report to best of your ability
3. Send to [INCIDENT RESPONSE TEAM LEAD] for review.
4. Once approved, remove this highlighting and send the report to [INCIDENT RESPONSE TEAM LEAD, TECHNICAL LEAD, DATA GOVERNANCE LEAD, LEGAL, COMMUNICATIONS, HR]

Issue Summary

Timeline

Root Cause

Resolution and recovery

Corrective and Preventative Measures

Good Fortune / Bad Fortune

What Worked / What Didn’t

Additional Comments

Issue Summary

Short summary (5 or fewer sentences):

1. *Summarize precipitating incident (example: Quickbooks server down due to a hardware failure or files unavailable due to a ransomware attack)*
2. *State the impact (example: email out for all staff for six hours, or 2.5GB of documents encrypted and unavailable for 4 hours)*

Timeline

Date, time, person that took action and result.

Root Cause

Give a detailed explanation of the event. DO NOT SUGARCOAT! Be cautious of blaming, but be candid and clear about what led to the incident.

Resolution and recovery

Provide a detailed explanation of actions taken and the timeline over which those actions took place.

Corrective and Preventative Measures

What changes do we recommend (if any) to mitigate risk/impact of future incidents of this type?

Good Fortune / Bad Fortune

Where did we get lucky or experience bad luck during the handling of this incident?

What Worked / What Didn’t

What controls/procedures in our system(s) and response(s) worked and which failed?

Additional Comments

If you have any additional comments not covered above, add them here.