secureframe

Build trust. Unlock growth.

Security Incident Response Plan Template

1. Purpose and Scope
2. Management
3. Incident Response Process
4. Testing
5. Exceptions
6. Enforcement
7. Responsibility, Review, and Audit

1 Purpose and Scope

The Security Incident Response Plan provides a systematic incident response process for all Information Security Incident(s) (defined below) that affect any of _____ **[COMPANY]**'s information technology systems, network, or data, including _____ **[COMPANY]** data held or services provided by third-party vendors or other service providers. From time to time, _____ **[COMPANY]** may update this policy and implement different levels of security controls for different information assets, based on risk and other considerations.

This plan applies to all _____ **[COMPANY]** assets utilized by personnel acting on behalf of _____ **[COMPANY]** or accessing its applications, infrastructure, systems or data. All personnel are required to read, accept and follow all _____ **[COMPANY]** policies and plans.

[COMPANY NAME] intends for this plan to:

- Define the security incident response process and provide step-by-step guidelines for establishing a timely, consistent, and repeatable incident response process.
- Assist _____ **[COMPANY]** and any applicable third parties (including vendors and partners) in quickly and efficiently responding to and recovering from different levels of information security incidents.
- Mitigate or minimize the effects of any information security incident on _____ **[COMPANY]**, its customers, employees, and others.
- Help _____ **[COMPANY]** consistently document the actions it takes in response to information security incidents.

“Information Security Incident” means an actual or reasonably suspected unauthorized use, disclosure, acquisition of, access to, corruption of, deletion, or other unauthorized processing of sensitive information that reasonably may compromise the privacy, confidentiality, integrity, or availability of that information.

2 Management

_____ **[COMPANY]** has an Incident Response Team (IRT) consisting of predetermined employees from key departments at _____ **[COMPANY]** to manage security incidents. The IRT provides timely, organized, informed, and effective response to information security incidents to (a) avoid loss of or damage to the _____ **[COMPANY]** systems, network, and data; (b) minimize economic, reputational, or other harms to _____ **[COMPANY]** and its customers, employees, contractors and partners; and (c) manage litigation, enforcement, and other risks.

The IRT also oversees and coordinates the development, maintenance and testing of the plan, its distribution, and ongoing updates of the plan. The Security Incident Response Plan is activated or enabled when a security incident occurs, and the IRT is responsible for evaluating the situation and responding accordingly. Depending on the severity of an incident the IRT may request engagement from various support teams to assist with the mitigation of the incident. The IRT meets on a periodic basis for training, education, and review of the documented plan.

The IRT consists of a core team with representatives from key _____ **[COMPANY]** groups and stakeholders.

The current IRT roster may be contacted at _____ **[SECURITY EMAIL]**.

3 Incident Response Process

The process outlined below should be followed by the appropriate Staff at _____ **[COMPANY]** in the event of an Information Security Incident. _____ **[COMPANY]** shall assign resources and adopt procedures to timely assess automated detection results, screen internal and external reports, and identify actual information security events. _____ **[COMPANY]** shall document each identified Information Security Incident.

Detection and Reporting

Automated Detection

_____ **[COMPANY]** may utilize automated detection means and other technical safeguards to automatically alert _____ **[COMPANY]** of incidents or potential incidents.

Report from Personnel

All _____ **[COMPANY]** personnel must report potential security incidents as follows:

- If you believe an incident occurred or may occur or may have identified a threat, vulnerability, or other security weakness, please report it to the following email immediately: ;
- Provide all available information and data regarding the potential incident; and
- Once an incident has been submitted, please stop using the affected system, or any other potentially affected device until being given the okay from the IRT

Report from External Source

External sources, including _____ **[COMPANY]**s customers, who claim to have information regarding an actual or alleged information security incident should be directed to _____ **[SECURITY EMAIL]** .

Employees who receive emails or other communications from external sources regarding information security incidents that may affect _____ **[COMPANY]** or others, security vulnerabilities, or related issues should immediately report those communications to and should not interact with the source unless authorized.

Response Procedures

Overview

Responding to a data breach involves the following stages:

1. Verification
2. Assessment
3. Containment and mitigation
4. Post-breach response

All of the steps must be documented in an incident log and/or corrective action plan.

The data breach response is not purely linear, as these stages and the activities associated with these stages frequently overlap. _____ **[COMPANY]** must keep a record of any actions the organization takes in responding to the incident and preserve any evidence that may be relevant to any potential regulatory investigation or litigation including through use of an incident log, corrective action plan or other applicable documentation.

(1) Verification

The IRT will work with _____ **[COMPANY]** employees and contractors to identify the affected systems or hardware (such as a lost laptop or USB drive) and determine the nature of the data maintained in those systems or on the hardware.

The IRT will determine the threshold at which events are declared a security incident and officially initiate the incident response process.

(2) Assessment

Following verification of an Information Security Incident, the IRT will determine the level of response required based on the incident's characteristics, including affected systems and data, and potential risks and impact to _____ **[COMPANY]** and its customers, employees, or others.

The incident assessment must include what employees or contractors were affected, what customers were affected, and what data was potentially exfiltrated, modified, deleted or compromised.

The IRT will work together to assess a priority with respect to the incident based on factors such as whether:

1. the incident exposed or is reasonably likely to have exposed data; or
2. personally identifiable information was affected and the data elements possibly at risk, such as name or date of birth.

In addition, the IRT will consider whether the disclosure was:

1. internal or external;
2. caused by a company insider or outside actor; and/or
3. the result of a malicious attack or an accident.

Lastly, if an information security breach has occurred, federal/country-wide law enforcement and local law enforcement should be contacted and informed of the breach. Law enforcement should be contacted in alignment with applicable breach notification laws. Internal and/or external general counsel should lead law enforcement communication efforts (in collaboration with IRT). If general counsel is not available, IRT should lead law enforcement communication efforts.

(3) Containment and Mitigation

As soon as _____ **[COMPANY]** has verified and assessed the breach, the IRT must take all necessary steps to contain the incident and return the _____ **[COMPANY]** systems back to their original state and limit further data loss or intrusion.

Such steps may include:

- Acting to stop the source or entity responsible, for example by:
- taking affected machines offline;
- segregating affected systems; or
- immediately securing the area if the breach involves a physical security breach.
- Determining whether other systems are under threat of immediate or future danger.
- Determining whether to implement additional technical measures to contain the data breach, such as changing locks, passwords, administrative rights, access codes, or passwords.

(4) Post-Breach Response

Any post-breach response including external and internal communications, notifications, and further inquiries will depend on the assessment and priority of the data breach.

As part of the final response based on the results of the breach, _____ **[COMPANY]** will review applicable access controls, policies and procedures and determine whether to take any actions to strengthen the organization's information security program.

Key Learnings

As soon as the incident has been resolved, _____ **[COMPANY]** senior management should meet with the IRT and other relevant team members of the _____ **[COMPANY]** for a post-mortem to better understand the incident that took place, and determine how similar incidents may be prevented in the future.

The retrospective should be documented and key learnings from the retrospective should be presented to all appropriate team members in a timely manner.

4 Testing

Testing the plan annually is critical to ensuring the plan is effective and practical. Any gaps in the plan that are discovered during the testing phase will be addressed by _____ **[COMPANY]** management. All tests must be thoroughly documented.

Testing of this plan may be performed using the following methods:

Walkthroughs

Team members walk through the steps documented in this plan to confirm effectiveness, identify gaps, bottlenecks or other weaknesses. This walkthrough provides the opportunity to review the plan with a larger subset of people, allowing the team to draw upon an increased pool of knowledge and experiences. Team members should be familiar with procedures, equipment, and offsite facilities.

Table Top Exercises

An incident is simulated so normal operations will not be interrupted. Scenarios of various security incidents are used and this plan is put into action to determine its use and effectiveness.

Validated checklists can provide a reasonable level of assurance for many of these scenarios. Analyze the output of the previous tests carefully before the proposed simulation to ensure the lessons learned during the previous phases of the cycle have been applied.

5 Exceptions

_____ **[COMPANY]** business needs, local situations, laws and regulations may occasionally call for an exception to this policy or any other _____ **[COMPANY]** policy. If an exception is needed, _____ **[COMPANY]** management will determine an acceptable alternative approach.

6 Enforcement

Any violation of this policy or any other _____ **[COMPANY]** policy or procedure may result in disciplinary action, up to and including termination of employment. _____ **[COMPANY]** reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. _____ **[COMPANY]** does not consider conduct in violation of this policy to be within an employee's or contractor's course and scope of work.

Any employee or contractor who is requested to undertake an activity that he or she believes is in violation of this policy must provide a written or verbal complaint to his or her manager or any other manager of _____ **[COMPANY]** as soon as possible.

The disciplinary process should also be used as a deterrent to prevent employees and contractors from violating organizational security policies and procedures, and any other security breaches.

7 Responsibility, Review, and Audit

This plan will be reviewed and tested on an annual basis. Ensuring that the plan reflects ongoing changes to resources is crucial. This task includes updating the plan and revising this document to reflect updates; testing the updates; and training personnel. Test results will be documented and signed off by _____ **[COMPANY]** management. The results are shared with appropriate parties internally and findings are tracked to resolution. Any changes are communicated across the organization.

This document is tested, maintained and enforced by _____ **[POLICY OWNER]** .

This document was last updated on _____ **[DATE MODIFIED]**.