

Incident Management Policy

Policy Owner

Approved by

Effective Date

Version

Next Review Date

1. Purpose

("**Company**") maintains this Incident Management Policy to establish a consistent process for identifying, reporting, assessing, responding to, resolving, documenting, and reviewing incidents that may affect the Company's people, operations, systems, information, property, customers, or legal and regulatory responsibilities.

This Policy is intended to reduce harm, support timely decision-making, preserve relevant information, and help the Company prevent similar incidents. It does not create a contract of employment or guarantee any particular response, outcome, or remedy.

2. Scope

This Policy applies to all Company personnel, including employees, officers, directors, temporary workers, contractors, consultants, interns, and other individuals who perform work for or on behalf of the Company.

This Policy applies to incidents involving Company operations, facilities, technology, data, products, services, vendors, customers, or business partners. It also applies where an incident occurs outside Company premises but may materially affect the Company.

3. Definitions

For purposes of this Policy:

Incident means an actual or suspected event that disrupts, threatens, or may disrupt Company operations, security, safety, confidentiality, integrity, availability, compliance obligations, or reputation.

Incident Manager means the individual appointed by the Company to coordinate the response to a specific Incident.

Incident Response Team means the group of personnel assigned to assess, contain, investigate, communicate about, and resolve an Incident.

Sensitive Information means information that requires protection under Company policy, contract, or applicable law, including personal information, confidential business information, financial information, authentication credentials, and proprietary information.

4. Policy Requirements

All personnel must promptly report actual or suspected Incidents through the reporting channels identified by the Company. Personnel must not delay reporting while attempting to investigate, resolve, or confirm an Incident independently.

The Company will assess reported Incidents, assign appropriate resources, and take response actions based on the nature, severity, potential impact, and urgency of the Incident. The Company may adjust its response as new information becomes available.

Personnel must cooperate with authorized Incident response activities, preserve relevant information, and follow instructions issued by the Incident Manager or Incident Response Team.

5. Reportable Incidents

Reportable Incidents include, but are not limited to:

- Unauthorized access to Company systems, accounts, facilities, or information
- Loss, theft, accidental disclosure, or improper handling of Sensitive Information
- Suspected phishing, malware, ransomware, or other security threats
- Significant system outages, service disruptions, or data loss
- Safety events, threats of violence, property damage, or environmental hazards
- Fraud, suspected misconduct, or material violations of Company policy
- Vendor, customer, or third-party events that may affect Company operations or information
- Any event that may require notice to customers, regulators, insurers, law enforcement, or other third parties

6. Incident Reporting

Personnel must report an Incident as soon as reasonably possible using . If the Incident presents an immediate threat to life, health, safety, or physical security, personnel should first contact applicable emergency services and then notify the Company through the designated reporting channel.

A report should include all known information, such as the date and time of the event, the systems, people, locations, or information involved, the actions already taken, and any available supporting records. Personnel should report in good faith even when information is incomplete.

The Company prohibits retaliation against any person who reports an Incident or participates in an Incident review in good faith.

7. Incident Classification and Prioritization

The Incident Manager or designated responder will classify the Incident based on its actual or potential impact, urgency, scope, and likelihood of escalation.

Severity Level	Description	Expected Response
Critical	The Incident causes or is likely to cause significant harm to people, major operational disruption, widespread exposure of Sensitive Information, or serious legal, financial, or reputational consequences.	Immediate escalation and coordinated response.
High	The Incident materially affects an important system, business process, customer group, or protected information but is not currently a Critical Incident.	Prompt investigation, containment, and leadership notification.
Moderate	The Incident has a limited or manageable impact and can be addressed through assigned operational or technical resources.	Timely response, documentation, and follow-up.
Low	The Incident has minimal impact and does not require urgent escalation.	Routine handling, tracking, and closure.

The Company may change an Incident’s severity level at any time as facts, impact, or risks change.

8. Incident Response Process

Upon receiving a report, the Company will take reasonable steps to validate the Incident, assess the potential impact, and assign an Incident Manager where appropriate.

The Incident Manager will coordinate response activities, identify required participants, establish response priorities, and maintain an Incident record. Depending on the circumstances, response actions may include containing the Incident, securing systems or locations, preserving evidence, restoring services, notifying affected parties, engaging outside specialists, and implementing corrective actions.

Response activities must be proportionate to the Incident and performed in a manner that protects affected individuals, preserves relevant information, and minimizes unnecessary disruption to business operations.

9. Roles and Responsibilities

The **Incident Manager** is responsible for coordinating the response, maintaining the Incident record, assigning response actions, escalating material issues, and confirming that closure requirements are met.

The **Incident Response Team** is responsible for carrying out assigned technical, operational, security, legal, compliance, human resources, communications, or customer-support actions.

Department Leaders must ensure that relevant personnel cooperate with Incident response activities and that corrective actions assigned to their departments are completed.

Personnel must promptly report suspected Incidents, preserve relevant information, avoid unauthorized public statements, and cooperate with authorized responders.

The Company may engage external legal counsel, forensic specialists, insurers, law enforcement, regulators, vendors, or other qualified third parties when appropriate.

10. Communications and Notifications

The Incident Manager will coordinate internal communications and, where necessary, recommend external notifications. Only authorized Company representatives may communicate with customers, the media, regulators, law enforcement, insurers, vendors, or other external parties about an Incident.

The Company will determine whether notification is required based on the facts of the Incident, contractual obligations, Company policy, and applicable legal requirements. Notifications will be made by the authorized function or individual and will contain information appropriate to the circumstances.

Personnel must not disclose Incident-related information except as necessary to perform assigned duties or as authorized by the Company.

11. Evidence Preservation and Confidentiality

Personnel must preserve relevant records, communications, logs, devices, files, photographs, access records, and other materials connected to an Incident. Relevant materials must not be altered, deleted, destroyed, or shared outside authorized channels.

Information relating to an Incident must be handled as confidential Company information and shared only with individuals who have a legitimate business need to know. The Company may restrict access to Incident records to protect privacy, legal interests, security, and the integrity of the review.

12. Recovery and Corrective Actions

The Incident Manager will coordinate recovery activities designed to restore affected operations safely and in an orderly manner. Recovery may include restoring systems, changing access credentials, repairing equipment, updating procedures, providing support to affected individuals, or taking other appropriate measures.

The Company will identify corrective actions reasonably necessary to address the root cause, contributing factors, or control gaps associated with an Incident. Assigned owners must complete corrective actions by the agreed deadline or promptly report any delay to the Incident Manager.

13. Post-Incident Review

For Critical and High Incidents, and for other Incidents when appropriate, the Company will conduct a post-incident review after stabilization. The review will assess the Incident's cause, impact, response effectiveness, communications, recovery actions, and opportunities for improvement.

The resulting record may include lessons learned, assigned corrective actions, responsible owners, and target completion dates. The purpose of the review is to improve Company processes and reduce the likelihood or impact of future Incidents.

14. Training and Testing

The Company may provide training, exercises, simulations, and other awareness activities to support effective Incident reporting and response. Personnel assigned Incident response responsibilities must complete any training designated by the Company for their role.

The Company may periodically test its Incident response procedures and update them based on test results, Incident reviews, changes in operations, or changes in risk.

15. Records Retention

Incident records must be created and maintained in accordance with the Company's record retention requirements and any applicable legal, contractual, or regulatory obligations. Records may include reports, evidence, decisions, communications, response actions, notifications, and post-incident reviews.

16. Noncompliance

Failure to comply with this Policy, including failure to report a known Incident, unauthorized disclosure of Incident information, interference with an investigation, or destruction of relevant information, may result in corrective action up to and including termination of employment or engagement, subject to applicable law and Company procedures.

17. Exceptions

Any exception to this Policy must be approved in writing by . An approved exception must describe its scope, duration, business justification, and any measures required to manage associated risks.

18. Policy Administration and Amendments

is responsible for administering this Policy and recommending updates. The Company may amend, replace, suspend, or withdraw this Policy at any time, subject to applicable law.

This Policy will be reviewed at least and more frequently when business operations, risk conditions, legal requirements, or material Incidents indicate that an update is appropriate.

19. Acknowledgment

By signing below, I acknowledge that I have received, read, and understand the Incident Management Policy. I agree to follow this Policy and to report actual or suspected Incidents promptly through the Company’s designated reporting channels.

Signatures

Company

Name

Date

Signature

Employee or Personnel

Name

Date

Signature



This document is a PDF copy of **Incident Management Policy** template. You can edit it with **Jotform Sign** and convert to an eSign document with **Jotform Sign**.

 **Edit PDF**

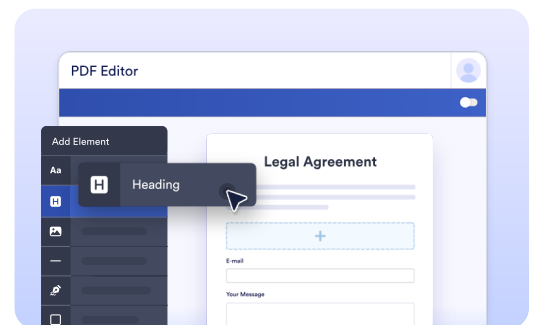
Learn More About Jotform PDF Products

Jotform offers powerful PDF solutions. Check them out below.

Jotform PDF Editor

Turn form submissions into PDFs automatically ready to download or save for your records.

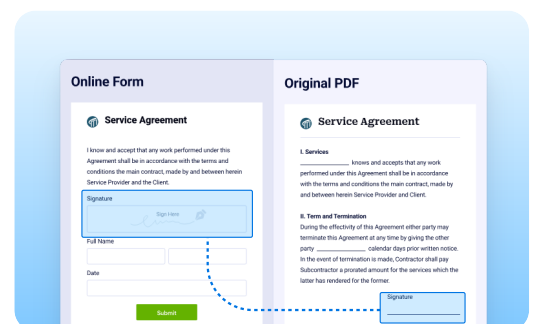
jotform.com/products/pdf-editor/



Smart PDF Forms

Convert your PDF files into online forms that are easy to fill out on any device.

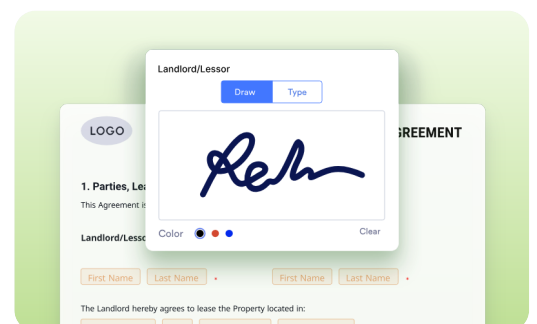
jotform.com/products/smart-pdf-forms/



Jotform Sign

Collect e-signatures with Jotform Sign to automate your signing process.

jotform.com/products/sign/



These templates are suggested forms only. If you're using a form as a contract, or to gather personal (or personal health) info, or for some other purpose with legal implications, we recommend that you do your homework to ensure you are complying with applicable laws and that you consult an attorney before relying on any particular form.