Incident Response Policy

Document Type	Internal Policy
Effective Date	
Version	
Approved by	
Last Review Date	

1. Purpose

This **Incident Response Policy** ("***Policy***") establishes a formal framework for identifying, reporting, assessing, managing, and resolving incidents that may impact ’s ("***Company***") operations, information assets, systems, personnel, or reputation. The purpose of this policy is to ensure that incidents are handled in a timely, coordinated, and consistent manner to minimize harm, restore normal operations, and support compliance with internal standards and applicable obligations.

2. Scope

This policy applies to all employees, officers, directors, contractors, consultants, temporary workers, and third parties who access or use Company’s systems, networks, facilities, data, or resources.

The policy covers all incidents affecting or potentially affecting:

- Information systems and technology assets
- Data confidentiality, integrity, or availability
- Physical facilities or equipment
- Business operations and service continuity
- Personnel safety or workplace integrity

3. Policy Authority and Status

This document is an internal policy of Company. It is intended to define procedures and responsibilities and does not create contractual rights or obligations unless expressly stated in writing. Compliance with this policy is mandatory for all individuals within its scope.

3. Policy Authority and Status

This document is an internal policy of Company. It is intended to define procedures and responsibilities and does not create contractual rights or obligations unless expressly stated in writing. Compliance with this policy is mandatory for all individuals within its scope.

4. Definitions

For the purposes of this Policy:

"Incident" means any actual or suspected event that disrupts, degrades, or threatens normal operations, security, safety, or data integrity.
"Security Incident" means an incident involving unauthorized access, disclosure, alteration, or destruction of information or systems.
"Incident Response Team ("*IRT*")" means the designated group responsible for coordinating incident response activities.
"Containment" means actions taken to limit the scope and impact of an incident.
"Recovery" means the process of restoring systems, services, or operations to normal or acceptable levels.

5. Incident Classification

Incidents may include, but are not limited to:

- Cybersecurity events such as malware, phishing, ransomware, or unauthorized access
- Data loss, data leakage, or suspected data compromise
- System outages or critical application failures
- Physical security breaches or equipment damage
- Workplace incidents affecting safety or compliance
- Third-party or vendor-related disruptions

Incidents may be classified internally by severity level (e.g., low, medium, high, critical) based on impact, urgency, and risk to the organization.

6. Incident Response Principles

All incident response activities shall be guided by the following principles:

- Prompt identification and reporting
- Proportional response based on severity and ris
- Clear accountability and documented decision-making
- Protection of personnel, data, and assets
- Preservation of evidence where required
- Continuous improvement through post-incident review

7. Roles and Responsibilities

All personnel must promptly report any actual or suspected incident in accordance with this policy and cooperate with response efforts. The Incident Response Team is responsible for coordinating incident handling, including assessment, containment, communication, and recovery activities. Management is responsible for providing oversight, approving escalation decisions, allocating resources, and supporting corrective actions. A designated coordinator may be assigned to manage communication, documentation, and task allocation during an incident.

8. Incident Reporting

Incidents must be reported as soon as they are identified or suspected through the designated reporting channels, such as:

- Internal ticketing or reporting system
- Designated email address or hotline
- Direct notification to management or IT/security personnel

Reports should include, where possible, a description of the incident, time of occurrence, affected systems or individuals, and any immediate actions taken.

9. Incident Response Process

Reported incidents are reviewed to confirm their nature, scope, and potential impact. Initial assessment determines severity and response priority. Appropriate steps are taken to limit further impact, such as isolating systems, restricting access, or suspending affected processes. The incident is analyzed to determine root causes, affected assets, and potential consequences. Evidence may be preserved where necessary. Systems, services, or operations are restored in a controlled manner. Recovery actions aim to resume normal operations while reducing the risk of recurrence. An incident is formally closed once remediation is complete and operations are stabilized.

9. Incident Response Process

Reported incidents are reviewed to confirm their nature, scope, and potential impact. Initial assessment determines severity and response priority. Appropriate steps are taken to limit further impact, such as isolating systems, restricting access, or suspending affected processes. The incident is analyzed to determine root causes, affected assets, and potential consequences. Evidence may be preserved where necessary. Systems, services, or operations are restored in a controlled manner. Recovery actions aim to resume normal operations while reducing the risk of recurrence. An incident is formally closed once remediation is complete and operations are stabilized.

10. Communication and Escalation

Significant incidents may require internal escalation to senior management or designated committees. External communication, including notifications to customers, partners, or authorities, must be approved by authorized personnel and coordinated through designated channels.

11. Documentation and Recordkeeping

All incidents and response actions must be documented, including timelines, decisions, actions taken, and outcomes. Records shall be retained in accordance with internal retention policies and applicable requirements.

12. Post-Incident Review

After resolution, a post-incident review may be conducted to evaluate response effectiveness, identify lessons learned, and recommend corrective or preventive measures. Findings may be used to update procedures, controls, or training.

13. Training and Awareness

Personnel with incident response responsibilities shall receive appropriate training. General awareness of reporting obligations and basic response expectations shall be communicated to all relevant personnel.

14. Policy Review and Amendments

This policy shall be reviewed periodically and may be updated to reflect organizational changes, risk assessments, or operational experience. Amendments must be approved by the appropriate authority and communicated to relevant stakeholders.

15. Non-Compliance

Failure to comply with this policy may result in corrective action in accordance with Company's internal procedures and applicable policies.

By approving this Policy, the undersigned confirms its adoption and authority for implementation.

Authorized Signatory

Name

Title

Date

Signature

Jotform

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

Edit PDF

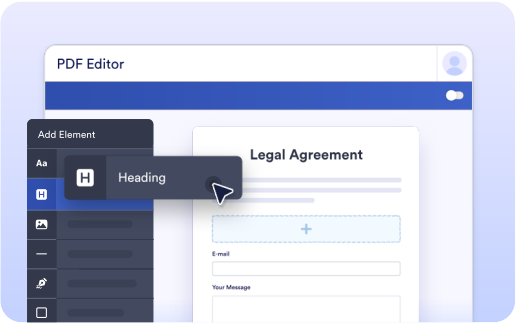
Learn More About Jotform PDF Products

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.

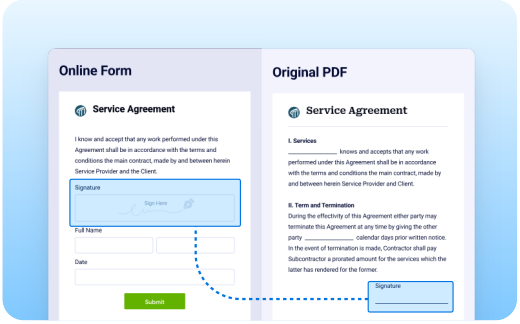
jotform.com/products/pdf-editor/



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/