IFIN Global Group

Incident Management Policy

1. Purpose

The purpose of this policy is to ensure a consistent and effective approach to managing incidents that threaten the security, integrity, or availability of IFIN Global Group's systems, data, or operations. This policy aims to minimize the impact of incidents on business functions and to maintain trust with stakeholders by responding promptly and effectively. It sets out the principles and responsibilities to guide incident management activities across the organization.

2. Scope

This policy applies to all employees, contractors, and third-party service providers who use or manage IFIN Global Group's IT resources. It encompasses all types of incidents, including but not limited to security breaches, data loss, system outages, and operational disruptions. The policy covers all locations and departments within the organization, ensuring a unified response to incidents.

3. Definitions

- **Incident:** An event that could lead to loss of, or disruption to, an organization's operations, services, or functions. Incidents can vary in severity and type, ranging from minor disruptions to major security breaches. Examples include unauthorized access, data leaks, hardware failures, and natural disasters affecting IT infrastructure.
- **Incident Management:** The process of identifying, analyzing, and correcting hazards to prevent a future re-occurrence. This involves a series of steps including detection, containment, eradication, recovery, and documentation, aimed at restoring normal operations and preventing future incidents.

4. Objectives

- To quickly and efficiently detect and respond to incidents, minimizing downtime and service disruption. The policy aims to establish clear procedures for incident response to ensure rapid action.
- To minimize the impact of incidents on operations, protecting the organization's assets and reputation. This involves implementing effective containment and mitigation strategies.
- To ensure timely communication to stakeholders, keeping them informed of incident status and resolutions. Transparency in communication helps maintain trust and manage expectations.
- To document incidents and the response to improve future incident handling, enabling continuous improvement in the incident management process. This includes learning from past incidents to enhance response capabilities.

5. Roles and Responsibilities

- **Incident Manager:** Oversees the incident management process and coordinates the response. The Incident Manager ensures that incidents are handled according to the policy and liaises with senior management.
- **Incident Response Team (IRT):** A group of experts who handle incidents, including IT staff, security personnel, and relevant department heads. The IRT is responsible for executing the incident management process and implementing technical and procedural solutions.
- **Employees:** Must report any suspected incidents to the Incident Manager or the helpdesk. Employees play a critical role in the early detection of incidents and must follow established reporting procedures promptly.

6. Incident Management Process

6.1 Identification

- **Detection:** Continuous monitoring of systems to detect anomalies. This involves using automated tools and manual checks to identify potential incidents as early as possible.
- **Reporting:** Immediate reporting of incidents through designated channels (helpdesk, email, incident management system). Quick reporting helps initiate a swift response and limits potential damage.

6.2 Categorization and Prioritization

- **Categorization:** Classify incidents based on type (e.g., security breach, system failure). Categorizing incidents helps in understanding their nature and required response.
- **Prioritization:** Assess the impact and urgency to prioritize response efforts. Prioritizing incidents ensures that resources are allocated to the most critical issues first.

6.3 Investigation and Diagnosis

- **Initial Assessment:** Determine the nature and extent of the incident. This step involves gathering initial information to understand the incident's scope.
- **Investigation:** Gather evidence, analyze the root cause, and assess the impact. A thorough investigation helps in identifying the source of the incident and preventing recurrence.

6.4 Resolution and Recovery

- **Containment:** Take immediate actions to contain the incident and prevent further damage. Containment strategies may involve isolating affected systems or implementing temporary fixes.
- **Eradication:** Remove the cause of the incident. This step focuses on eliminating the root cause to ensure the incident does not reoccur.
- **Recovery:** Restore affected systems and services to normal operation. Recovery efforts aim to bring operations back to normalcy with minimal disruption.

6.5 Closure

- **Documentation:** Record details of the incident, actions taken, and lessons learned. Comprehensive documentation provides a record for future reference and learning.
- **Review:** Conduct a post-incident review to identify improvements. Reviews help in evaluating the effectiveness of the response and identifying areas for improvement.

7. Communication Plan

- **Internal Communication:** Regular updates to relevant stakeholders and management. Keeping internal stakeholders informed ensures alignment and coordinated efforts.
- **External Communication:** Notify affected customers and regulatory bodies as required. Transparent communication with external parties helps manage expectations and comply with legal obligations.

8. Training and Awareness

- Regular training for all employees on incident identification and response procedures. Training programs ensure that employees are equipped to recognize and respond to incidents effectively.
- Awareness programs to keep staff informed about current threats and best practices. Ongoing awareness initiatives help maintain a high level of vigilance and preparedness.

9. Continuous Improvement

- Periodic reviews of the incident management process. Regular assessments help in keeping the process relevant and effective.
- Incorporate feedback from post-incident reviews and simulations (e.g., drills). Continuous improvement efforts focus on learning from past experiences and enhancing response capabilities.

10. Compliance and Legal Requirements

- Ensure compliance with relevant laws, regulations, and industry standards. Adhering to legal and regulatory requirements helps in avoiding penalties and maintaining a good reputation.
- Regular audits to verify adherence to this policy. Audits ensure that the policy is being followed and helps in identifying gaps for improvement.

11. Policy Review

- This policy will be reviewed annually or after a significant incident to ensure its continued relevance and effectiveness. Regular reviews help in adapting the policy to evolving threats and organizational changes.