## Incident Response Plan

| | |
|---|---|
| **Version** | **2023/02.01** |
| **Review Date** | **22/03/2024** |
| **Review & Approved by** | **Reviewed by Technology Committee & Approved by Board of Directors** |

### 1.0 Overview

This incident response plan defines what constitutes a security incident and outlines the incident response phases. It includes the roles and responsibilities of the Chief Information Security Officer (CISO) in handling security incidents. The plan covers incident assessment, damage minimization, response strategies for different types of attacks, documentation, evidence preservation, and reporting procedures to both internal and external stakeholders. The plan aims to ensure a structured and coordinated approach to incident response.

### 2.0 Purpose

The purpose of this policy is to protect organizational resources against intrusion by establishing clear guidelines and procedures for incident response. It aims to mitigate the impact of security incidents, restore business continuity, prevent future incidents, improve security measures, and keep management informed about the situation and response. Additionally, it outlines the reporting procedures for both internal and external stakeholders to ensure timely and effective communication.

### 3.0 Incident Response Goals

The incident response plan is designed to achieve the following goals:

1. Verify that an incident has occurred.
2. Maintain or restore business continuity.
3. Minimize the impact of the incident.
4. Determine the cause and method of the attack or incident.
5. Implement preventive measures to mitigate future incidents.
6. Enhance security measures and incident response capabilities.
7. Facilitate legal prosecution of illegal activities.
8. Keep management informed about the incident and response efforts.
9. Ensure timely and effective reporting to both internal and external stakeholders.

### 4.0 Incident Definition

An incident is defined as any of the following:

1. Loss of information confidentiality (data theft).
2. Compromise of information integrity (data damage or unauthorized modification).
3. Theft or damage to physical IT assets, including computers, storage devices, and printers.
4. Denial of service attacks.

For, Genuine Stock Brokers Pvt. Ltd.

Manager / Director

5. Misuse of services, information, or assets.
6. Infection of systems by unauthorized or malicious software.
7. Attempted unauthorized access.
8. Unauthorized changes to organizational hardware, software, or configurations.
9. Reports of unusual system behavior.
10. Responses to intrusion detection alarms.

### 5.0 Incident Planning

In the incident response plan, the following steps should be taken to ensure effective incident handling:

1. Roles and Responsibilities:
    - Chief Information Security Officer (CISO): Responsible for overall incident response coordination, incident assessment, and decision-making.
    - Incident Response Team: Comprises members responsible for specific tasks such as technical analysis, containment, eradication, and recovery.
    - Communication Officer: Responsible for internal and external communication during and after an incident.
2. Procedures:
    - Specific procedures for different types of incidents, such as viruses, hacker intrusions, data theft, or system destruction are given in Annexure 1.
    - Consider the criticality of the affected systems or data.
    - Differentiate between ongoing and completed incidents.

### 6.0 Incident Response Lifecycle

1. Incident Preparation:
    - Define computer security policies, incident response procedures, and backup and recovery procedures.
    - Implement security tools like firewalls and intrusion detection systems.
    - Conduct user training on computer security and train IT staff in handling security situations.
    - Establish contact lists and emergency procedures.
    - Test the incident response process.
2. Discovery:
    - Incidents can be discovered through various sources such as helpdesk, intrusion detection systems, system administrators, or reports from partners or monitoring teams.
3. Notification:
    - Use the emergency contact procedure to notify the incident response team, including the CISO.
4. Analysis and Assessment:
    - Evaluate the incident based on factors like its reality, current progress, data or asset threats, impact on the business, and targeted systems.
5. Response Strategy:
    - Determine the urgency and containment measures required for an effective response.
    - Implement specific response strategies based on the type of attack, such as isolating affected systems, changing passwords, or blocking connections.
6. Containment:

    - Take immediate action to prevent further intrusion or damage.
    - Disconnect affected systems, change passwords, block suspicious ports or connections, and isolate the incident.

7. Prevention of Re-infection:
    - Investigate the intrusion source and take steps to prevent re-infection.
    - Close vulnerable ports, apply patches, reinstall infected systems, and enhance security measures.
8. Restore Affected Systems:
    - Restore affected systems to their original state while preserving evidence against the intruder.
    - Reinstall systems from scratch, restore data from backups, enforce password changes, harden systems, and ensure up-to-date security measures.
9. Documentation:
    - Document incident details, response actions, and their effectiveness.
    - Keep records of how the incident occurred, the attack source, and the response effort.
10. Evidence Preservation:
    - Make copies of relevant logs, emails, and other communication.
    - Maintain lists of witnesses and preserve evidence for potential legal actions.
11. Notifying Proper External Agencies:
    - Notify the appropriate external agencies, such as law enforcement, if legal action is possible.
12. Assess Damage and Cost:
    - Assess the damage to the organization, estimate the cost of containment efforts, and evaluate the impact on business operations.
13. Review Response and Update Policies:
    - Review the effectiveness of the incident response process.
    - Identify areas for improvement in policies, procedures, and preventive measures.
    - Update security policies based on lessons learned from the incident.

## 7.0 Reporting Procedures

Internal Reporting:

- The Chief Information Security Officer (CISO) shall be promptly informed about any security incident.
- The incident response team should document the incident details, response actions, and their outcomes.
- Regular status updates should be provided to management and relevant stakeholders.

External Reporting:

- Incidents involving data breaches, cyber attacks, or regulatory violations should be reported to the appropriate external entities.
- Follow the reporting guidelines provided by regulatory bodies, such as the Securities and Exchange Board of India (SEBI) or Computer Emergency Response Team (CERT-In).
- Provide incident reports to the external entities within the specified timeframes and through designated channels.

- Maintain clear records of all external incident reports for future reference.

## 8.0 Review and Update

This policy shall be reviewed and updated on an annual basis or on any special event or circumstance.

Annexure 1: Procedures for Different Types of Incidents

1 Virus Incident Procedure:

1. Detection: a. Identify signs of a potential virus infection, such as system slowdowns, unusual pop-ups, or unexpected system behaviour. b. Immediately report any suspicious activity to the incident response team.
2. Containment: a. Isolate the affected system(s) from the network to prevent further virus propagation. b. Disable network connections and disconnect from external devices. c. Activate real-time virus protection and initiate a system scan to identify and quarantine the infected files.
3. Eradication: a. Remove the virus from the system by using up-to-date antivirus software. b. Perform a thorough system scan to ensure all infected files and remnants are eliminated. c. Update antivirus signatures and definitions regularly.
4. Recovery: a. Restore clean versions of infected files from reliable backups. b. Validate the integrity of the restored files to ensure they are free from infections. c. Reinstate network connectivity after verifying the system's security.
5. Prevention: a. Educate users on safe browsing habits, email attachment best practices, and downloading software from trusted sources. b. Implement email filtering to prevent the delivery of suspicious attachments or links. c. Regularly update software and operating systems with the latest patches and security updates.

2 Hacker Intrusion Incident Procedure:

1. Detection: a. Monitor intrusion detection systems and network logs for any suspicious or unauthorized activities. b. Conduct regular vulnerability assessments and penetration tests to identify potential vulnerabilities. c. Train employees to recognize and report phishing attempts or social engineering attacks.
2. Containment: a. Isolate the affected systems or compromised accounts to prevent further unauthorized access. b. Change passwords for compromised accounts and implement multi-factor authentication. c. Identify the extent of the intrusion and determine the affected systems or data.
3. Eradication: a. Identify the entry point and close any security gaps or vulnerabilities. b. Remove any malicious software or backdoors left by the attacker. c. Analyse system logs and network traffic to identify any unauthorized modifications or data exfiltration.
4. Recovery: a. Restore affected systems from clean backups or rebuild them from scratch if necessary. b. Strengthen security measures, such as implementing stronger access controls and regular security updates. c. Conduct post-incident penetration tests to ensure the network's resilience against future attacks.

5. Prevention: a. Regularly update and patch systems, applications, and firmware to address known vulnerabilities. b. Implement network segmentation and strong firewall configurations to limit lateral movement. c. Conduct security awareness training to educate employees about social engineering attacks and the importance of safe computing practices.

3 Data Theft Incident Procedure:

1. Detection: a. Monitor network logs, data access patterns, and unusual user activities. b. Implement data loss prevention (DLP) solutions to detect and prevent unauthorized data exfiltration. c. Conduct regular audits and data integrity checks to identify any suspicious changes.
2. Containment: a. Isolate the compromised systems or accounts to prevent further data exfiltration. b. Disable compromised accounts and change passwords for affected users. c. Identify the scope of the data breach and the sensitive information that might have been compromised.
3. Investigation: a. Preserve evidence by capturing system logs, network traffic, and any relevant information related to the data breach. b. Engage forensic experts, if necessary, to determine the extent of the breach and identify the perpetrators.
4. Notification and Reporting: a. Comply with legal and regulatory requirements for reporting data breaches to the appropriate authorities and affected individuals. b. Notify affected individuals promptly and provide guidance on protecting themselves from potential harm. c. Document the incident, including the timeline, affected systems, and steps taken for containment and recovery.
5. Recovery and Mitigation: a. Restore affected systems from clean backups and validate the integrity of recovered data. b. Enhance data protection measures, including encryption, access controls, and monitoring solutions. c. Conduct security awareness training to educate employees about data protection and handling sensitive information.

4 System Destruction Incident Procedure:

1. Detection: a. Monitor system logs and security alerts for any signs of unauthorized system destruction attempts. b. Implement intrusion detection systems and behavioural analytics to identify abnormal system behaviour.
2. Containment: a. Isolate affected systems from the network to prevent further damage. b. Preserve system logs, backups, and any available evidence for forensic analysis.
3. Investigation: a. Engage forensic experts to determine the cause and extent of the system destruction. b. Identify the attacker's methods and motives behind the incident.
4. Recovery and Restoration: a. Rebuild affected systems from scratch or restore them from secure backups. b. Validate the integrity and security of restored systems and data. c. Implement enhanced security measures, including intrusion prevention systems and regular vulnerability scanning.
5. Prevention: a. Implement access controls and least privilege principles to limit unauthorized access to critical systems. b. Regularly backup critical data and store backups securely offline or in an isolated network segment. c. Conduct periodic security assessments to identify and remediate vulnerabilities that could lead to system destruction.

Genuine Stock Brokers Pvt. Ltd. * Ahmedabad