“Incident Response Plan (IRP)”

Company: DAS TECHNOLOGY SERVICES LLC
Author: Shaheer Nawaz, IT Support Specialist
Review Cycle: Annual
Version: V1.1
Approved By: IT Security Department

1.Introduction

The purpose of this Incident Response Plan (IRP) is to provide a structured approach for detecting, responding to, and recovering from security incidents, while minimizing the impact on business operations and ensuring the protection of data, including T-Mobile’s sensitive information. This plan applies to all company systems, networks, and users.

---

1. Objectives

- To detect, assess, and respond to incidents in a timely and efficient manner.
- To limit damage and prevent further exploitation of vulnerabilities.
- To ensure timely recovery and restoration of services.
- To comply with relevant legal and regulatory requirements.
- To learn from incidents to improve future response and defenses.

---

2. Incident Response Team (IRT)

The Incident Response Team is responsible for managing and resolving security incidents. The team consists of the following members:

- **Incident Response Manager**: Oversees incident response activities, ensures communication, and reports to management.
- **Security Analysts**: Identify and analyze the incident, provide technical analysis, and execute containment and eradication actions.

- **IT Support Team**: Implements technical recovery measures and ensures the restoration of systems.
- **Legal/Compliance Officer**: Handles legal aspects and ensures compliance with data protection laws, including breach notifications.
- **Public Relations/Communications**: Manages internal and external communications regarding the incident.

---

3. Incident Classification

Incidents are classified based on their severity and type, which helps prioritize response efforts. The primary categories are:

- **Low Severity**: Minor incidents that pose minimal threat to the business (e.g., false alarms, limited system disruptions).
- **Medium Severity**: Moderate incidents that may affect operations but can be contained within a short time frame (e.g., malware infections, unauthorized access).
- **High Severity**: Major incidents with potential data breaches or prolonged operational disruptions (e.g., ransomware attacks, data leaks).

---

4. Incident Response Phases

Phase 1: Detection s Identification

- **Monitoring Tools**: Continuously monitor systems using automated tools (SIEM, EDR) to identify signs of security incidents.
- **Initial Report**: Any employee or system can report a potential incident via our internal incident reporting tool or helpdesk.
- **Incident Logging**: All incidents are logged with detailed information including the time of detection, potential impact, and the initial assessment.

Phase 2: Containment

- **Short-term Containment**: Implement immediate measures to isolate affected systems and prevent the spread of the incident (e.g., disconnecting network access, disabling compromised accounts).
- **Long-term Containment**: Apply more lasting solutions, such as restricting further access or implementing additional safeguards.

Phase 3: Eradication

- **Root Cause Analysis**: Identify the cause of the incident (e.g., malicious software, configuration error).
- **System Cleanup**: Remove all traces of the incident from systems (e.g., deleting malware, closing vulnerabilities).

- **Patch s Secure**: Apply security patches or configuration changes to prevent similar incidents from occurring.

Phase 4: Recovery

- **Restoration of Services**: Gradually restore affected systems to full functionality, ensuring that they are secure and fully patched.
- **Monitoring**: Implement heightened monitoring for any signs of recurrence or additional attacks.
- **Communication**: Keep stakeholders (including T-Mobile, if applicable) informed about recovery progress and system status.

Phase 5: Post-Incident Review

- **Incident Analysis**: Perform a detailed post-mortem analysis to understand what happened, how the response was handled, and what could be improved.
- **Report Generation**: Generate a report summarizing the incident, response actions, lessons learned, and any changes made to prevent recurrence.
- **Improvement Plans**: Update security policies, procedures, and tools based on the lessons learned.

---

5. Reporting and Communication

- **Internal Communication**: Maintain clear communication channels with all stakeholders during an incident.
- **External Reporting**: If applicable, notify external parties such as T-Mobile, law enforcement, or regulatory bodies, according to contractual and legal requirements.
- **Breach Notification**: If the incident involves a data breach, promptly notify T-Mobile in accordance with our contractual obligations, including details on the breach and actions taken.

---

6. Documentation s Recordkeeping

- All incident actions, including detection, response steps, and decisions made, will be documented in real-time.
- Incident logs and reports will be retained for audit and compliance purposes.

7. Plan Testing and Training

- The incident response plan will be tested annually through tabletop exercises and simulated incident scenarios to ensure readiness.
- All relevant personnel will undergo regular training on their roles and responsibilities within the incident management process.

G. Conclusion

This Incident Response Plan provides a framework to ensure that any security incidents are handled quickly and effectively, minimizing damage and maintaining compliance with contractual and regulatory obligations, including those related to T-Mobile's data.