Incident Response Plan

Date: 17/03/2025

V: 2

Approved by

General Manager

Jamal Kubeer

شركة شبكة الخدمات الآلية
Automated Services Network Co.

Contents

Purpose:

The purpose of this incident plan is to outline procedures and responsibilities for responding to security incidents at Automated Services Network Co. With a dedicated IT Network and Security team, we aim to minimize the impact of incidents on operations, safeguard physical and digital assets and maintain trust.

The plan covers detection, assessment, containment and recovery procedures, along with roles and communication guidelines. Regular review and training ensure an effective response and a culture of security awareness. By implementing this plan, we demonstrate our commitment to maintaining security standards and business continuity in the face of evolving threats.

Scope:

The policy applies to all Automated Services Network Co. employees and stake holders. It encompasses security incidents involving information technology infrastructure, applications, and data assets owned or operated by Automated Services Co.

The plan covers incidents occurring within Automated Services Network Co's Network environment, including but not limited to unauthorized access, data breaches, malware infections, denial-of-service attacks, and insider threats. Additionally, this plan extends incidents impacting cloud-based services. It is designed to ensure a consistent and coordinated response to security incidents across all areas of the organization, facilitating effective incident management and mitigation efforts.

Maintenance:

The organization's cyber security specialist is responsible for the maintenance and revision of this document.

Authority:

The General Manager has the authority to determine when to activate and execute the Incident Response Plan in response to security incidents affecting Automated Services Network Co. Upon notification or detection of a security incident, the General Manger will assess the situation, and make the decision to initiate the incident response process as necessary.

Incident Response Team:

The incident response team consists of employees within the organization who will take part in an incident response execution based on their roles and responsibilities.

1. **General Manager:**
   - Taking the decision to execute the incident response plan.
   - Collaborating closely with internal stakeholders to ensure alignment with organizational objectives.

- Coordinating communication with external parties such as regulatory authorities.

- Overseeing resource allocation for response efforts and leading the post-incident review process to identify lessons learned and enhance incident response capabilities.

2. HR Manager:

- Coordinating internal communication regarding the incident, ensuring the employees are informed about the situation, any impact on their work, and any actions the need to take.

- Ensuring that the incident response activities adhere to relevant HR policies, such as those related to employee confidentiality, data protection, and employee rights during investigations.

- Organization training sessions and awareness programs to educate employees about their roles and responsibilities in incident response.

- Assisting in documenting incident response activities related to personnel, including keeping records of employee communications, actions taken, and any HR-related incidents or issues arising from the incident.

3. Cyber Security Specialist:

- Identify indicators of compromise IOCs and anomalous behavior to initiate incident response procedures promptly.

- Ensure that response procedures are documented, up-to-date, and aligned with industry best practices and regulatory requirements.

- Assess the severity and impact of security incidents based on available information, risk assessments, and organizational priorities. Prioritize response efforts to address critical incidents promptly and efficiently.

- Lead efforts to contain security incidents and prevent further unauthorized access or data loss. Implement security controls, such as firewall rules, access controls, and network segmentation, to mitigate the impact of incidents and prevent their recurrence.

- Develop and deliver training sessions, workshops, and awareness programs to educate employees about cybersecurity best practices, incident response procedures, and emerging threats

4. **Senior Network and Security Engineer:**
   - Detecting and analyzing security incident affecting the organization's network infrastructure, systems and applications.
   - Conducting Analysis to determine the root cause of the incident, the extent to compromise and any artifacts left behind by the attacker.
   - Gather and Preserve evidence for further investigation.

5. **Software Developers:**
   - Identifying and patching the vulnerabilities, fixing code exploits and restoring affected systems to a secure start.
   - Reviewing and analyzing code to identify potential security vulnerabilities or weaknesses that may have contributed to the incident.
   - Developing and deploying patches or updates to software applications and systems identified during incident response activities.
   - Implementing lessons learned from security incidents to secure coding practices, architecture reviews, and threats modeling exercises to proactively identify and mitigate security risks in software development processes.

Incident Classification:

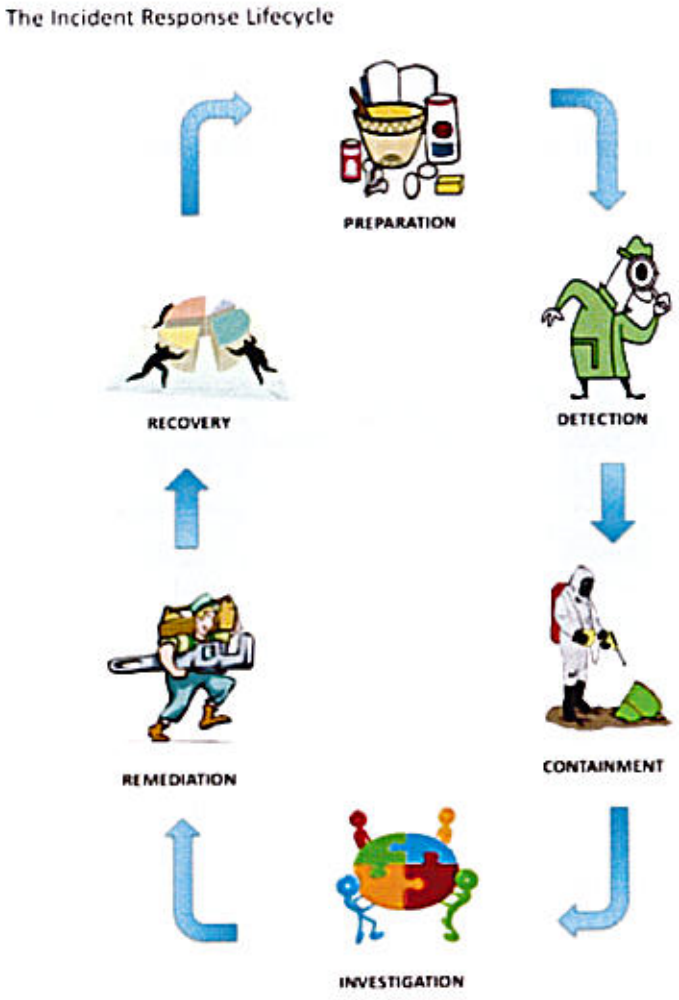
The security incidents will be classifieds according to the severity and the impact caused to the environment.

Level 1	Low Severity	Minor impact on operations, systems or data	Incident does not pose an immediate threat to security	Low-risk vulnerabilities, minor system glitches, isolated phishing attempts with no successful compromises
Level 2	Medium Severity	Moderate impact on operations, systems, or data, potentially affecting productivity	Incident requires attention and mitigation within reasonable timeframe to prevent escalation	Limited data exposure, successful malware infections on individual systems, unauthorized access to non-critical resources
Level 3	High Severity	Significant impact on operations, systems, or data resulting in disruptions,	Incident requires immediate attention and mitigation to minimize impact	Ransomware attacks causing widespread data encryption, network breaches compromising sensitive information,

		downtime or loss of critical information	and restore operations	denial-of-service (DoS) attacks affecting critical services
Level 4	Critical Severity	Impact: Severe and widespread impact on operations, systems, or data, posing a significant risk to business continuity, financial loss, or reputation damage	Incident demands immediate and decisive action to contain, mitigate, and recover from the incident.	Data breaches exposing highly sensitive information (e.g., PII, financial records), advanced persistent threats (APTs) compromising core infrastructure, zero-day vulnerabilities with active exploitation

Incident Response Phases:

The incident response process encompasses six phases: Preparation, detection, containment, investigation and recovery. There phases are defined in (NIST SP 800-61, 2024).



Preparation:

Policies, tools, procedures, effective governance and communication plans. Preparation also implies that the affected groups have instituted the controls necessary to recover and continue operations after an incident is discovered. Post-mortem analyses from prior incidents should form the basis for continuous improvement of this stage.

Detection:

Detection is the discovery of the event with the security tools or notification by network security and network security specialist about a suspected incident. This phase includes the declaration and initial classification of the incident, as well as any initial notifications required by law or contract.

Containment:

Containment is the triage phase where the affected host or system is identified, isolated or otherwise mitigated and when affected parties are notified and investigative status established. This phase includes sub-procedures for seizure and evidence handling, escalation, and communication.

Investigation:

Investigation is the phase where the incident response team members determine the priority, scope, risk and root cause of the incident.

Remediation:

Remediation is the post-incident repair of affected systems, communication and instruction of affected parties, and analysis that confirms the threat has been remediated. Any determination of regulatory requirements and all internal and external communications are determined by key stakeholders. Apart from any formal reports, the post-mortem will be completed at this stage as it may impact the remediation and interpretation of the incident.

Recovery:

Recovery is the analysis of the incident for its procedural and policy implications, the gathering of metrics and the incorporation of "lessons learned" into future response activities and training.

Escalation:

At any time during the incident response process, the General Manager may be called upon to escalate any issue regarding the process or incident.

Revision History

Version	Date	Author	Signature
1.0	17-March-2025	Cyber Security Officer	U. Rama Krishna