

4.9.1 Incident Management Policy

Contents

1. Definitions	3
2. Purpose	3
3. Scope	3
4. Policy	4
5. Non-compliance	5
6. References	6

File Classification: **Restricted** - Internal Use



Document approval:

Version	Adjustment Date	Approved By	Approval Date and signature
2.1	15/7/2025	CEO Saud Alsulami	16/7/2025

Previous document information:

Version	Adjustment Date	Modified by	Reasons for modification
2.1	15/7/2025	Cybersecurity officer	Modification of Security Event Classification
2.0	15/4/2024	Cybersecurity officer	Policy improvements
1.1	3/2023	Cybersecurity officer	Improved on status
1.0	2/2024	Cybersecurity officer	Create



1. Definitions

For purposes of this "Incident Management Policy" the following definitions apply:

- **Security incidents:** events or occurrences that potentially jeopardize the confidentiality, integrity, or availability of an organization's information assets.
- **Security Incident Response Committee:** a group or team within an organization responsible for coordinating and managing the response to security incidents.
- **Eradication:** the process of permanently removing or eliminating the root cause of a security incident or vulnerability from the organization's systems, networks, or infrastructure.
- **Root causes:** the underlying factors or primary reasons that contribute to the occurrence of security incidents or vulnerabilities within an organization's environment.

2. Purpose

This policy sets out the framework for managing information security incidents within Taqnyat Al-Jawal. Ensure timely and effective response to minimize losses, maintain business continuity and comply with relevant regulations.

3. Scope

This policy applies to all employees, contractors and third-party service providers who have access to Taqnyat's information systems and assets. It covers all types of information security incidents, including:

- Unauthorized access or disclosure of confidential information
- Interruption or loss of information system availability
- Data leakage or corruption
- System malfunction or malfunction
- Denial-of-service attack
- Malware infection



4. Policy

- 4.1. All employees of Taqnyat are required to report any security incidents to the cybersecurity department.
- 4.2. All clients of Taqnyat are requested to report any security incidents to the technical support department.
- 4.3. The technical support department is required to report any security incident communicated by customers to the cybersecurity department and relevant departments within a maximum period of 24 hours.
- 4.4. Security incidents must be reported through the approved communication channels of Taqnyat (email, phone).
- 4.5. The cybersecurity officer must continuously monitor the logs and take proactive measures to protect against any security event.
- 4.6. Incident reports should include details such as the nature of the incident, date/time, potential impact, and any relevant evidence.
- 4.7. When receiving any security incident, the cybersecurity department evaluates the incident with the Security Incident Response Committee, which consists of the NOC department and the technical advisor.
- 4.8. Security incidents are handled according to the Security Incident Management Plan
- 4.9. The Security Incident Management Plan should include the following steps:
 - Containment: Taking actions to minimize the impact of the incident, such as isolating compromised systems.
 - Eradication: Identifying and eliminating the root cause of the incident.
 - Recovery: Restoring normal operations and affected data.
 - Preservation of Evidence: Collecting and preserving evidence for potential forensic investigation.



- 4.10. Security incidents should be addressed based on their classification according to the following timeframes:
- **Limited/Low Incidents:** These should be addressed within 10 working days from the date of reporting or discovery of the incident.
 - **Medium Incidents:** These should be addressed within 5 working days from the date of reporting or discovery of the incident.
 - **High Incidents:** These should be addressed within 1 working day from the date of reporting or discovery of the incident.
 - **Critical Incidents:** These should be addressed within 2 hours from the date of reporting or discovery of the incident.
 - **Catastrophic Incidents:** These should activate the BCP plan
- 4.11. The Security Incident Response Committee, while handling any security incident, communicates with all relevant departments and top management. If necessary, they also engage with relevant regulatory authorities.
- 4.12. The cybersecurity manager will analyze the causes of the security incident to discover the factors that led to it while dealing with the security incident.
- 4.13. After dealing with the security incident, the cybersecurity officer will evaluate the effectiveness of the response to analyze and improve it if necessary and benefit from it in future training on dealing with security incidents.
- 4.14. The findings from the review must be documented and used to update the incident management plan and improve future response capabilities.
- 4.15. After resolving the security incident, the cybersecurity department must submit a report to the senior management, including recommendations that must be taken to avoid such incidents in the future.

5. Non-compliance

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment, and related civil or criminal penalties.



6. Reviews

This policy will be reviewed annually, and the review schedule is as follows:

Review Date	Reviewed By
25/12/2024	Cybersecurity officer

7. References

- ISO 27002
- ISO 27001

