3.1.1 Cybersecurity Risk Assessment Policy

Contents

Version	Adjustment Date	Approved By	Approval Date
2.0	18/12/2025	Saud Alsulami	2/1/2025

1. Definitions

For purposes of this “Cybersecurity Risk Assessment Policy” the following definitions apply:

- **Risk assessments:** are systematic processes used to identify, analyze, and evaluate potential risks that could affect the achievement of objectives within an organization. In the context of cybersecurity, risk assessments involve identifying and understanding the potential threats, vulnerabilities, and impacts associated with information systems and data.
- **Risk Mitigation:** The process of prioritizing, implementing, and maintaining appropriate measures to reduce cybersecurity risk to an acceptable level.
- **Risk Acceptance:** The decision to take no action against a particular risk and accept the outcome of its potential impact.
- **Risk Transfer:** The process of formally shifting the financial consequences of certain risks to another party, typically through insurance or outsourcing.

2. Purpose

This policy establishes the framework for conducting cybersecurity risk assessments within Taqnyat Corporation. Its aim is to identify, evaluate, and prioritize risks to the organization's information assets, ensuring the protection of these assets, individuals, and other organizations potentially impacted by our operations.

3. Scope

The policy applies to all information systems, networks, and data used or managed by Taqnyat Corporation. It covers risks related to cyber threats, data breaches, technology failures, and human factors. The assessment extends to third-party services and vendors whose operations impact our information security.

4. Policy

4.1. The risk assessment must consider all aspects of Taqnyat’s information systems, including hardware, software, data, personnel, and physical security.

4.2. The risk assessment must consider the asset classifications.

4.3. Potential threats (both internal and external) a[illegible] aqnyat’s information systems must be identified.

4.4. The likelihood and potential impact of identified risks shall be assessed.

4.5. Risks must be prioritized based on their severity and the value of the affected assets.

4.6. Comprehensive documentation of the risk assessment process, findings, and recommended risk mitigation strategies is required.

4.7. Strategies to mitigate high-priority risks must be developed. These may include technical controls, policy changes, training programs, or contingency plans.

4.8. Relevant stakeholders must be involved in the risk assessment process. This includes IT staff, management, and where necessary, external experts.

4.9. Assessments shall consider compliance with relevant cybersecurity laws, regulations, and industry standards.

4.10. Decisions regarding risk acceptance or transfer must be documented where risks cannot be mitigated.

4.11. Procedures for ongoing monitoring of identified risks and the effectiveness of implemented controls are required.

4.12. The risk assessment process must be regularly reviewed and updated to reflect changes in the threat landscape, business operations, and technological environment.

4.13. Frequency for Risk Assessment

- Regular Assessments: Risk assessments shall be conducted annually as a standard practice.
- Triggered Assessments: Additional assessments will be triggered by:
  - Significant changes in the IT infrastructure or business processes.
  - Introduction of new technologies or decommissioning of existing ones.
  - After a major security incident or data breach.
  - Changes in compliance requirements or legal regulations.
  - Recommendations from previous risk assessments.
  - launching new products

4.14. The Chief Information Security Officer (CISO) is responsible for the implementation and oversight of this policy.

4.15. The cybersecurity risk assessment should be aligned with the company's comprehensive risk assessment. The risk register should be shared with the company's risk assessors.

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. References

- ISO 27005
- National Cybersecurity Authority's (NCA) ECC standards
- NIST