4.11.1 Information Protection Policy

Contents

Version	Adjustment Date	Approved By	Approval Date
2.0	4/7/2024	Saud Alsulami	7/7/2024

1. Definitions

For purposes of this “Information Protection Policy” the following definitions apply:

- **Information Assets:** Any data, document, or information owned, managed, or held by Taq Company.
- **Classification Level:** The categorization of information based on its sensitivity and criticality (e.g., restricted, confidential, public).
- **Personally Identifiable Information (PII):** Information that can be used to identify an individual, either alone or when combined with other information.
- **Data at Rest:** Data that is stored on a physical or electronic medium.
- **Data in Transit:** Data that is being transmitted across a network.
- **Data in Use:** Data that is currently being processed.

2. Purpose

The purpose of this Information Protection Policy is to establish a comprehensive framework for the protection of Taqnyat Company's information assets. This policy aims to ensure the confidentiality, integrity, and availability of information by defining requirements for information classification, privacy, ownership, protection, transmission, and retention. The policy also ensures compliance with relevant cybersecurity standards and regulations.

3. Scope

This policy applies to all employees, contractors, consultants, and any other individuals or entities that have access to Taqnyat Company's information assets. It covers all forms of information, including electronic, paper, and verbal communication, across all departments and business units.

4. Policy

4.1. Classification Levels and Criteria:

- Confidential: This information is classified as confidential and can only be viewed with the approval of the owner. It must not be leaked or published inside or outside the company. Leaking this information poses a high risk to the company. This includes financial and accounting data.

- Internal: This information is classified as for internal company use only. It can be viewed by employees but cannot be leaked or circulated outside the company

without the approval of the owner or general manager. This includes policies and procedures followed within the company.

- Public: This information is classified as public and can be published and circulated without any risk. This includes information found on the company's website.

4.2. Privacy, Ownership, Protection, Transmission, and Retention:
- Privacy: Ensure the privacy of PII and other sensitive information through appropriate access controls and data handling practices.
- Ownership: Define clear ownership of information assets as per assets discovery policy to ensure accountability and responsibility for data protection.
- Protection: Implement security measures to protect information at rest, in transit, and in use, including encryption as per encryption policy and access controls as per Permission Matrix.
- Transmission: Secure the transmission of information using encryption and secure communication protocols.
- Retention: According to the information disposal policy, customer information is disposed of after one year.

4.3. Data Protection:
- Data in Transit: Use encryption and secure communication protocols (e.g., TLS, VPN) to protect data during transmission.
- Data at Rest: Encrypt sensitive information stored on physical or electronic media.
- Data in Use: Implement measures to protect data during processing, such as secure coding practices and runtime encryption.

4.4. Information disposal
- Confidential and internal data, whether physical or electronic, is disposed of according to the safe data disposal policy, which includes subscriber, financial, and accounting data.

4.5. Information use:
- Information must not be used in a way that could affect the company's reputation and operations.
- Real customer information must not be used in the test environment. Instead, special test data prepared internally must be used.

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 27002
- National Cybersecurity Authority's (NCA) ECC standards