

2.4.1 Acceptable Use of Information Assets

Contents

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

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

1. Definitions

For purposes of this “Acceptable Use of Information Assets” the following definitions apply:

- **Information Assets:** This refers to all digital information, software, and systems that are valuable to the organization, including but not limited to data, databases, applications, networks, and computers.
- **Acceptable Use:** The permitted and intended utilization of information assets for legitimate business purposes.
- **Unauthorized Use:** Any use of information assets that violates company policies, guidelines, or legal regulations.
- **Removable Media:** Portable storage devices that can be easily connected to and removed from a computer, such as USB drives, external hard drives, and memory cards.

2. Purpose

The purpose of this policy is to establish guidelines for the acceptable use of information assets within Taqnyat. This policy aims to protect the Taqnyat's information assets, ensure secure usage, and maintain the integrity and confidentiality of sensitive information.

3. Scope

This policy applies to all employees, contractors, and authorized users who have access to the company's information assets, including but not limited to computers, networks, software, and data.

4. Policy

- 4.1. Acceptable Use: Information assets provided by the company should be used for legitimate business purposes only. Unauthorized use, including personal gain or illegal activities, is strictly prohibited.



- 4.2. Prohibited Activities: Users must not engage in any activities that compromise the security or integrity of information assets. This includes but is not limited to the installation of unauthorized software, unauthorized access to web pages, and the use of removable media for non-business purposes.
- 4.3. Web Access: Access to web pages should be in alignment with the Taqnyat's business needs and employees' job responsibilities. Personal use of the internet should be minimal and not interfere with work-related tasks.
- 4.4. Web Access Control: Taqnyat Company reserves the right to control internet access, monitor usage, and block access to specific websites that may pose a threat to the company's assets and information. The NOC team, with the approval of the CEO, will take the necessary actions to enforce this policy.
- 4.5. Software Installation: Only authorized software approved by the IT department can be installed on company devices. Users must not install any unwanted or unlicensed software.
- 4.6. Removable Media: The use of removable media, such as USB drives or external hard drives, is permitted only when necessary for business purposes. All data stored on removable media must be encrypted and protected in accordance with the Taqnyat's data protection policies.
- 4.7. Classification and Handling of Information: All information assets should be classified based on their sensitivity and criticality to the organization. Users must handle information in accordance with its classification, ensuring that confidential and sensitive information is protected and accessed only by authorized individuals.
- 4.8. Secure User Behavior: Users are responsible for maintaining secure behavior when using information assets. This includes adhering to password policies, not sharing credentials, reporting suspicious activities, and being vigilant against social engineering and phishing attempts.
- 4.9. Incident Reporting: All suspected or confirmed security incidents, breaches, or violations of this policy must be reported immediately to the cybersecurity officer. Users should be aware of the incident reporting procedures and provide all relevant information to facilitate prompt investigation and resolution.

- 4.10. Access Control and User Provisioning: Access to information assets should be based on the principle of least privilege. User accounts and access rights should be provisioned, reviewed, and revoked in a timely manner to ensure that only authorized users have access to the information they need.
- 4.11. Secure Configuration and Patch Management: Information assets, including operating systems, software applications, and network devices, should be securely configured and regularly patched to prevent vulnerabilities and exploits. Users must not modify or bypass security configurations.
- 4.12. Mobile Device and Remote Access Security: Users accessing company information assets from mobile devices or remote locations must comply with the company's mobile device management policies and remote access guidelines. This includes the use of approved devices, encryption, strong authentication, and regular security updates.
- 4.13. Physical and Environmental Security: Users must maintain the physical security of information assets and their surroundings. This includes securing workstations, protecting against unauthorized access, and adhering to environmental guidelines, such as temperature and humidity controls, to prevent damage or disruption to assets.
- 4.14. Supplier and Third-Party Relations: When engaging with suppliers or third-party service providers who have access to company information assets, users must ensure that these parties adhere to the company's security policies and standards. Contracts and agreements should include appropriate security clauses and requirements.

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
- ISO 27001
- National Cybersecurity Authority's (NCA) ECC standards



Internal Use Only