

5.4.1 Network Security

Contents

1. Definitions	2
2. Purpose	2
3. Scope	3
4. Policy	3
5. Non-compliance	5
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 "Network Security" the following definitions apply:

- **Network Security:** Network security refers to the policies, processes, and practices designed to protect the organization's networks, systems, and data from unauthorized access, use, disclosure, disruption, modification, or destruction. It involves securing the network infrastructure, devices, and data transmitted over the network.
- **Information Assets:** Information assets refer to any data, systems, or devices that are valuable to the organization and are connected to or impacted by the network.
- **Traffic Control:** Traffic control involves monitoring, managing, and controlling all incoming and outgoing network traffic to prevent unauthorized or malicious activity.
- **Firewall:** A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between a trusted network and untrusted networks, blocking unauthorized access while allowing legitimate traffic to pass through.
- **Encryption:** Encryption is the process of converting data into a secure, unreadable format (ciphertext) that can only be accessed by authorized users with the correct decryption key. Encryption ensures the confidentiality and integrity of sensitive information transmitted over networks.
- **Network Segregation:** Network segregation, also known as network segmentation, involves dividing a network into smaller, isolated segments or zones based on factors such as function, sensitivity of data, or criticality of systems. This reduces the potential impact of a security breach and improves overall network security.
- **Access Control:** Access control refers to the policies, procedures, and technical controls that regulate who or what can access network resources and data. It involves authenticating and authorizing users, devices, or processes before granting access to network systems or information assets.
- **DDoS (Distributed Denial of Service) Attack:** A DDoS attack is a malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming it with a flood of Internet traffic, making it unavailable to legitimate users.

2. Purpose

The purpose of this policy is to outline the requirements, responsibilities, and procedures for maintaining the security of Taqnyat's networks and the information assets connected to them. This policy aims to protect the Taqnyat's network

infrastructure, ensure the confidentiality, integrity, and availability of data, and prevent unauthorized access, use, or disruption of our networks.

3. Scope

This policy applies to all employees, contractors, and third parties who have access to or impact the security of Taqnyat's networks. It covers all network devices, systems, and services owned, operated, or used by Taqnyat, including but not limited to firewalls, routers, switches, wireless access points, and telecommunications systems. This policy also applies to all information assets connected to Taqnyat's networks, including servers, workstations, and mobile devices.

4. Policy

4.1. Traffic Control and Monitoring:

- All incoming and outgoing network traffic shall be controlled and monitored based on the defined Requirements for Network Security. This includes preventing malicious traffic, detecting and mitigating DDoS attacks, and controlling unwanted communication such as spam emails or unauthorized SMS messages.
- Firewalls and intrusion prevention systems shall be used to block unauthorized protocols and IP addresses, and to disable unused protocols, reducing the attack surface.
- Access to the wired network is prohibited across all branches of the Taqnyat.
- Taqnyat network access is granted by adding the MAC address to the existing Wi-Fi systems and the relevant VLAN.
- Employees are permitted to access the Guest network, which is entirely isolated and does not provide access to Taqnyat's systems; it only allows for internet browsing.

4.2. Information Protection:

- Data transmitted over Taqnyat's networks shall be protected from unauthorized interception, copying, or modification. Encryption protocols shall be employed to ensure the confidentiality and integrity of sensitive information.
- Virtual Private Networks (VPNs) shall be used for remote access to internal networks, ensuring secure connections and data trans



4.3. Network Segregation:

- Taqnyat's networks shall be segregated into zones based on the criticality and sensitivity of the information assets and services. This includes isolating production networks from development and testing environments, and separating user workstations from authentication servers.
- Firewalls and access control lists shall be used to restrict and control communication between different network zones.

4.4. Telecommunications Security:

- Taqnyat shall secure all data, voice, and signaling information transmitted over its telecommunications network, including SMPP.
- The organization's hosted customer networks shall be logically segregated from its own operational network, ensuring customer data privacy and security.

4.5. Network Resilience:

- Taqnyat shall implement measures to handle internal and external attacks, such as DoS/DDoS attacks, including the use of distributed denial of service (DDoS) mitigation services.
- To avoid network congestion and service disruptions, additional facilities shall be implemented to balance traffic loads and detect potential congestion issues.

4.6. Network Monitoring and Analysis:

- Specific tools and techniques shall be employed to analyze and filter network traffic, detecting and blocking unauthorized or malicious traffic. This includes port filtering, host-based filtering, and behavioral analysis.
- Regular vulnerabilities assessments shall be conducted to identify and remediate potential vulnerabilities.

4.7. Continuous Improvement:

- The Requirements for Network Security shall be continuously measured, reviewed, and optimized to ensure their effectiveness and alignment with industry best practices and standards.
- All employees with network responsibilities shall receive regular training on network security practices and stay updated on emerging threats and countermeasures.
- The network diagram should be created, reviewed, and amended every six months to reflect any modifications made to the network.

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 27011
- SANS v7.0
- National Cybersecurity Authority's (NCA) ECC/ CSCC standards

