

2.3.1 Bring Your Own Device (BYOD)

Contents

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

Version	Adjustment Date	Approved By	Approval Date and signature
2.1	18/12/2025	Saud Alsulami	2/1/2025



1. Definitions

For purposes of this “Bring Your Own Device (BYOD)” the following definitions apply:

- **Personally Owned Mobile Device:** Any mobile device, such as smartphones, tablets, or laptops, that is owned by an individual employee and not provided by Taqnyat.
- **PIN (Personal Identification Number):** A numeric code or password used as an authentication mechanism to access a mobile device.
- **Encryption:** The process of converting data into a secure format to prevent unauthorized access or data breaches.

2. Purpose

The purpose of the Bring Your Own Device (BYOD) Policy is to establish guidelines for the secure use of personally owned mobile devices within Taqnyat. This policy aims to protect sensitive data, ensure compliance with security standards, and maintain a secure environment.

3. Scope

This policy applies to all employees, contractors, and third parties who are granted the privilege to use personally owned mobile devices for work-related purposes within the Taqnyat organization.

4. Policy

4.1. The connection of any device not owned by the company to any of the company's resources is not permitted. However, the use of personally owned mobile devices to connect to the Taqnyat network is a privilege granted exclusively to employees and only upon formal approval by CEO.

4.2. Personally owned laptop devices must meet the following security requirements:

- Have approved virus and spyware detection/protection software installed and activated.
- Enable personal firewall protection.

4.3. Access to Taqnyat email via mobile devices requires the use of a PIN or strong authentication mechanism for enhanced security.

4.4. Employees must ensure the isolation of personal information from work-related information on their mobile devices to protect both personal and work-related data.



- 4.5. Confidential information may only be stored on devices that are encrypted in compliance with the Taqnyat Encryption Standard.
- 4.6. In the event of theft or loss of a mobile device containing confidential or internal information, employees must immediately report the incident to the Taqnyat Security Team.
- 4.7. All mobile devices must maintain up-to-date versions of operating systems, software, and applications to promptly address security vulnerabilities.
- 4.8. Taqnyat IT Management may perform remote wipes of mobile devices without warning in cases of suspected incidents or breaches to protect sensitive data.
- 4.9. IT support for personally owned mobile devices is limited to assisting users in complying with this policy. Troubleshooting for device usability issues may not be provided.
- 4.10. The use of personally owned devices must adhere to all other Taqnyat policies.
- 4.11. Upon completion of work on personal devices, the technical support department must ensure that the information is securely deleted in such a way that it cannot be recovered again
- 4.12. This policy shall be reviewed annually

5. Non-compliance

Non-compliance with this policy may result in disciplinary actions, including but not limited to warnings, suspension of mobile device privileges, or termination of employment, as determined by Taqnyat management.

6. References

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

