

6.1.1 Cloud Services Policy

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
1.1	17/06/2025	Saud Alsulami	17/06/2025

1. Definitions

For purposes of this “Cloud Services policy” the following definitions apply:

- **Cloud Service Provider (CSP):** A third-party company that offers cloud-based services, including infrastructure, platforms, or software, to organizations or individuals.
- **Identity and Access Management (IAM):** A set of processes and technologies that ensure only authorized individuals have access to specific resources or systems within an organization.
- **Service Level Agreement (SLA):** A formal agreement between a service provider and a customer, outlining the expected level of service, including performance metrics, availability, and responsibilities.
- **Uptime Percentage:** The percentage of time a system, service, or infrastructure is operational and available for use, often used to measure the reliability of services.

2. Purpose

The policy aims to ensure the secure and reliable utilization of cloud services for hosting on-premises equipment, safeguarding data integrity, and maintaining compliance with standards.

3. Scope

This policy applies to all personnel involved in the management, utilization, and oversight of on-premises equipment hosted in the cloud, outlining cybersecurity requirements, service level agreements, and responsibilities to mitigate risks and enhance operational resilience.

4. Policy

Taqnyat utilizes cloud service providers to host its infrastructure. Therefore, it is essential to choose a cloud service provider that fulfills the following criteria:

- 4.1. Cloud providers must adhere to recognized industry cybersecurity standards (e.g., ISO 27001) to ensure a robust security framework.
- 4.2. All data transmitted between Taqnyat, and the cloud service provider must be encrypted using strong, accepted encryption algorithms.

- 4.3. The cloud service provider must implement access control measures for the infrastructure of the technology company and monitor these procedures.
- 4.4. Cloud providers must have documented incident response procedures, and Taqnyat should be notified promptly in case of any security incidents affecting its data.
- 4.5. The cloud service provider shall respond to any incidents within a timeframe defined by the SLA.
- 4.6. Cloud providers must comply with data protection and privacy regulations as needed by the CST.
- 4.7. The cloud service provider must commit to providing services within the Kingdom of Saudi Arabia
- 4.8. The SLA must define the minimum acceptable level of service availability. Ensure that the cloud provider commits to a specific uptime percentage and establish procedures for reporting and handling downtime incidents.
- 4.9. The SLA must clearly outline the process for terminating the use of cloud services and retrieving the Taqnyat equipment.
- 4.10. The SLA or contract must include termination methods, as well as the Taqnyat's right to conduct audits at any time to ensure compliance with requirements, in coordination with host providers
- 4.11. An annual review of policies is conducted.
- 4.12. A risk assessment for the use of hosting services must be conducted and reviewed annually

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

