táaleem
inspiring young minds

Cybersecurity Policy

Policy Details

Policy Title	Cybersecurity Policy
Policy Number	IT-007
Policy Owner	IT Department
Version	1
Effective Date	01 May 2026
Scheduled Review Date	30 April 2028
Applicable To	All

Prepared by:

Name	Designation	Signature
Wael Omar	Director of IT	Signed by: Wael Omar 72511DCC0A694E7...

Reviewed by:

Name	Designation	Signature
Natasha Pardasani	Head of Compliance	DocuSigned by: Natasha Pardasani 0D63CBA9319B4B2...

Approved by:

Name	Designation	Signature
Sam Truman	Chief Operating Officer	DocuSigned by: D70E6514BCA94A6...
Alan Williamson	Chief Executive Officer	Signed by: A88F8F28883242C...

Table of Contents

1. Purpose

This policy establishes the framework by which Taaleem Holding P.J.S.C (hereafter referred to as "Taaleem" or the "Company") secures its information systems, data, and digital assets. It ensures the confidentiality, integrity, and availability of information while safeguarding staff, students, and corporate operations in compliance with UAE regulations and Taaleem's responsibilities as a listed company.

2. Scope

This policy applies to all Taaleem staff, students, third parties and vendors who use Taaleem-owned or managed IT systems, applications, and networks.

3. Guiding Principles

- Confidentiality, integrity, and availability of systems and data must be preserved.
- Cybersecurity is a shared responsibility across the Group.
- Safeguarding students in the digital environment is a core principle.
- Compliance with regulatory and contractual obligations is mandatory.

4. Roles & Responsibilities

- **Board of Directors** shall provide strategic oversight of cybersecurity risk and receive periodic reporting on the organisation's cyber risk posture.
- **Senior Executive Board (SEB) / C-Suite** shall ensure that appropriate resources and governance structures are in place to support the cybersecurity programme.
- **Director of IT** shall be accountable for policy implementation, compliance monitoring, and reporting to the Senior Executive Board.
- **Central Office IT function** shall implement, operate, and maintain security controls in line with this policy and approved procedures.
- **System Owners and Data Owners** shall approve access to business-critical or sensitive applications.
- **All staff** shall comply with this policy and promptly report security incidents in line with the Cybersecurity Incident Response Plan within the Emergency and Crisis Management Policy.

5. Regulatory Compliance

This Cybersecurity Policy is informed by relevant UAE regulatory frameworks, including Federal Decree-Law No. (34) of 2021 on Countering Rumours and Cybercrimes, where applicable.

6. Definitions:

- Microsoft Entra ID: The system Taaleem uses to manage user sign-ins and control access to applications and data.
- Multi-Factor Authentication (MFA): A security method that requires more than one form of verification to access systems or data.
- Mobile Device Management (MDM): A system used to secure and manage mobile devices that access Taaleem systems or data.
- Virtual Local Area Network (VLAN): A method of dividing a network into secure groups to improve security and performance.
- Software-Defined Wide Area Network (SD-WAN): A technology that securely connects multiple locations over the internet.
- Software as a Service (SaaS): Software that is hosted by a provider and accessed over the internet.
- Security events: Logged activities or alerts that indicate potential security issues or incidents.

7. Policy Requirements

Identity & Access Management

- Access must be provisioned through Microsoft Entra ID with role-based access control (RBAC) and least-privilege.
- Access must be provisioned according to the user's role and business need.
- Access to business-critical applications requires documented approval from the relevant system owner.
- Multi-factor authentication (MFA) is mandatory for staff; students are exempt in line with Microsoft education best practice.
- Conditional access policies are applied as required to manage risk.
- User access reviews are performed bi-annually by Central Office IT and system owners, with evidence retained to support internal and external audit requirements.

Segregation of Duties & Privileged Access

- Administrative and privileged access are restricted and separated so that no individual can independently execute critical system or data changes without oversight.

Infrastructure & Network Security

- All endpoints must be managed through mobile device management (MDM) with encryption, patching, and baseline configurations enforced.
- Network traffic must be segmented using Virtual Local Area Network (VLANs) (corporate, student, guest, IoT) with policy-based assignment through centralized controls.
- Perimeter firewalls and Software-Defined Wide Area Network (SD-WAN) are centrally managed, with configuration changes logged and retained.
- All Taaleem systems and SaaS platforms must enforce encryption for data at rest and in transit.

Threat Protection & Email Security

- Advanced threat protection is applied to email and collaboration platforms.
- Microsoft Defender technologies (Safe Attachments, Safe Links) are enabled to block phishing, malware, and malicious URLs.
- Protection extends across Outlook, Teams, SharePoint, and OneDrive.
- Phishing simulation exercises are conducted quarterly to build user resilience.

Vulnerability & Patch Management

- All on-premises systems must be patched on a scheduled basis. Security updates are applied monthly, with patching occurring on the last Friday of each month, unless a critical vulnerability requires expedited action.
- For SaaS platforms, patching is the responsibility of the vendor and assurance must be obtained through contractual commitments or published updates.

Monitoring & Incident Response

- Security events are centrally monitored for suspicious activity, with alerts investigated by Central IT.
- Incidents shall be managed in line with the cybersecurity incident response procedures outlined in the Emergency & Crisis Management Policy.
- An independent external penetration test is conducted annually, on an approved scope with remediation actions tracked to closure.

Third-Party & Vendor Security

- Third-party vendors and service providers that process, store, or access Taaleem data under contract are expected to apply and maintain appropriate security controls.
- Vendors are responsible for implementing security measures to safeguard Taaleem SaaS data; ultimate accountability for safeguarding remains with Taaleem as the data owner.
- Taaleem shall monitor vendor compliance, where applicable, by requesting evidence of compliance (e.g., SOC reports, bridge letters, ISO 27001 certificates, GDPR compliance, etc.), which vendors are expected to provide upon request.

Privacy & Data Protection

- Personal data is governed by Taaleem's Data Protection Policy.
- Cybersecurity controls listed in this policy must be integrated to safeguard student and staff data.
- Breaches must be reported in line with the Emergency and Crisis Management Policy, UAE law and regulatory obligations.

Awareness & Culture

- Cybersecurity awareness training is mandatory for all staff[1] and shall be in accordance with the yearly Cyber Security Awareness Programme for Taaleem.
- Phishing awareness campaigns and simulations are conducted quarterly.
- Digital safeguarding measures and literacy programs are embedded for staff based on the cybersecurity awareness programme on a yearly basis.

Log Retention & Protection

- Audit logs must be enabled on all critical systems and applications where technically feasible. Retention periods shall align with the capabilities of each platform, with a minimum baseline of 30 days as per IT Retention timelines.

Threat Intelligence & Contact with Special Interest Groups

- Threat intelligence is actively sourced from trusted and relevant channels to support early identification, risk analysis, and proactive response to cybersecurity threats. Taaleem maintains engagement with recognised special interest groups, industry forums, and professional associations to stay current with emerging threats, evolving tactics, and cybersecurity best practices.

[1] To be implemented for all staff post H2 of FY 25/26.

Cybersecurity Metrics & Reporting

- Key cybersecurity metrics (e.g., phishing simulation results, penetration testing outcomes, incident trends) are reported periodically to SEB, while control validation and effectiveness are assured through audit and internal control reviews and formally reported to the Audit Committee.

Policy Integration

- This policy must be read in conjunction with related governance documents, including:
  - Data Protection Policy.
  - Change Management Policy.
  - IT Disaster Recovery Plan.
  - Enterprise Risk Management Framework.
- Together, these documents form the cybersecurity and IT risk governance framework for Taaleem.

8. Policy Exceptions

Where a specific cybersecurity control defined in this policy cannot be fully implemented due to a technical, operational, or business constraint, a formal exception may be requested through the following process:

1. The exception must be submitted in writing to the Information Security Manager, with a clear description of the control that cannot be met, the reason, the associated risk, and proposed compensating controls.

2. The exception must be reviewed and approved by the Director of IT. Where the risk is assessed as high or critical, escalation to the COO is required prior to approval.

3. All approved exceptions must be time-bound, with a maximum duration of six months, after which they must be formally renewed or closed.

4. A register of all active exceptions, including their status, risk rating, compensating controls, and expiry date, must be maintained by the Information Security Manager and made available to the Compliance function and internal / external auditors upon request.

5. Exceptions do not exempt the relevant team or individual from the obligation to remediate the underlying gap within the approved timeframe.

9. Implementation Timeline

This policy shall be implemented within thirty (30) days from the Effective Date indicated on the cover page, allowing adequate time for communication, training, and adoption across all relevant Taaleem entities (if not implemented already). Where any requirement in this policy is dependent on a system functionality, configuration, or tool that is not yet implemented, such requirement shall take effect only once the relevant functionality is operational. Until such time, existing processes shall continue to apply.

10. Non-Compliance

Non-compliance with any established corporate policies may result in disciplinary action.

Version Control

Version No.	Date	Details of Changes
1	May 2026	Initial version of the Cybersecurity Policy

Disclaimer:

This document and its contents are the confidential and proprietary information of Taaleem Holdings PJSC and its subsidiaries. Any unauthorised access, distribution, or reproduction of this document is strictly prohibited.