Greenwich University

Policy Title:	**DATA AND CYBER SECURITY POLICY**		
Custodial Office:	Registrar Office	Policy Number:	GU/SKM-R/2021-88/13
Policy Contact:	Registrar Office	Date Approved:	February 21, 2026
Approved By:	Academic Council	Date of Issue:	March 02, 2026
Related Documents:	GU Policy Manual	Next Review:	February 2028
Revision:	Every two years		

N.B: ***This policy may be amended at any time without prior notice. All revisions shall supersede any previous versions and shall take effect immediately upon approval.***

QUALITY ENHANCEMENT CELL

GREENWICH UNIVERSITY

1. Purpose

The purpose of this policy is to establish a framework for securing Greenwich University's digital assets, including administrative, academic, and research data. It ensures the confidentiality, integrity, and availability of data, mitigates cybersecurity risks, and aligns with Higher Education Commission (HEC) standards, including PERN connectivity and Jidar framework guidelines.

2. Scope

This policy applies to all:

- Students, faculty, staff, and contractors of Greenwich University
- University-owned IT infrastructure, networks, and applications (ERP, Learning Management System, email, cloud storage)
- Research and administrative data, including AI-generated datasets

3. Policy Principles

3.1 Data Classification

All data shall be classified according to sensitivity:

1. **Highly Sensitive:** Research data, personally identifiable information (PII), financial records, intellectual property
2. **Confidential:** Internal administrative data, HR records, student grades
3. **Non-sensitive / Open:** Public information, course syllabi, marketing materials

3.2 Access Control

- Access to data will be role-based, with minimum privileges necessary for job functions.
- Multi-Factor Authentication (MFA) is mandatory for ERP, email, cloud storage, and administrative portals.
- All users must authenticate using official Greenwich University credentials.

3.3 Data Storage and Residency

- University data must be stored **on** approved servers: private cloud, RAID-backed storage, or governed cloud services (e.g., Microsoft 365 / OneDrive).
- Local storage on personal laptops or USB drives is prohibited unless explicitly authorized by the IT department.
- Research data must be backed up off-site to prevent accidental loss.

3.4 Research Data Security

- All research data shall follow HEC retention guidelines (minimum 3–5 years post-publication).
- Sensitive research data cannot be uploaded to public AI platforms without anonymization and IT approval.
- Export of research data for remote work requires encrypted, IT-approved devices.

3.5 AI Data Governance

- AI tools must not be used for data fabrication, plagiarism, or exposure of sensitive information.
- Departments must maintain logs of AI tool usage and data input to monitor compliance.

3.6 Network and Infrastructure Security

- All network devices must be protected with firewalls, WPA3/WPA2-Enterprise Wi-Fi, and endpoint security.
- University servers must run anti-malware software with regular updates and patch management.
- Virtualized environments (Hyper-V) must follow segregation policies to prevent cross-VM data leakage.

3.7 Incident Response

- Security incidents (data breaches, ransomware attacks, unauthorized access) must be reported immediately to the **IT Security Officer**.
- The university shall maintain a **Security Operations Center (SOC)**, either on-premises or via HEC/PERN integration, for 24/7 monitoring.
- An **incident response plan** will be enacted to investigate, contain, and remediate breaches.

3.8 Compliance and Auditing

- Internal audits will verify compliance with this policy annually.
- Non-compliance may lead to disciplinary action, including suspension of IT privileges.
- Greenwich University will adhere to HEC Cyber Security Guidelines, Pakistan Cloud First Policy, and PERN connectivity standards where applicable.

4. Roles and Responsibilities

Role	Responsibilities
Director IT / IT Security Officer	**Implement security controls, maintain SOC, conduct audits, approve data access**
Department Heads	**Ensure departmental compliance, report incidents, manage AI usage logs**
Faculty / Researchers	**Classify research data, use secure storage, follow AI governance**
Students / Staff	**Protect login credentials, report suspicious activity, follow approved device usage**

5. Training and Awareness

- Annual cybersecurity and data privacy training is mandatory for all staff and students.
- Specialized workshops will cover secure use of AI tools, data anonymization, and incident reporting.

6. Policy Review

- This policy will be reviewed **every two years** or earlier if required due to regulatory changes, emerging threats, or IT infrastructure updates.
- Revisions must be approved by the Registrar Office and published to all university stakeholders.