جامعة فهد بن سلطان
FAHAD BIN SULTAN UNIVERSITY

Official Email and Work Data Storage Policy

Policy #:	IT-930	Revision #:	01
Accessibility level:	Internal	Effective date:	Oct.2026

1. Purpose

This policy requires that all official FBSU communication and all work data remain within systems that FBSU owns, controls and can audit, in order to protect personal data, keep official records complete, and keep FBSU data subject to the laws of the Kingdom of Saudi Arabia.

2. Scope

This policy applies to all faculty, staff, contractors, vendors and programmers, and to students when they act on behalf of the University. It covers all email and messaging used for official business, and all FBSU data in any form, on any device or service.

3. Official Email

3.1. **FBSU accounts only:** All official communication must be sent and received through an @fbsu.edu.sa account. Using Gmail, Hotmail, Outlook.com, Yahoo or any other non-FBSU email for official business is **prohibited**. This includes communication with students, applicants, parents, staff, vendors, partner institutions and government entities.

3.2. **No forwarding:** Automatic or manual forwarding of FBSU email to a personal or external address is prohibited. The IT Center disables external auto-forwarding at tenant level.

3.3. **Messaging apps:** Personal messaging apps (WhatsApp, Telegram and similar) must not be used to send Confidential or personal data, official decisions, documents or records. Brief coordination messages are permitted only if they contain no such data; all other communication must use the official channels approved by the IT Center (FBSU email, FBSU Teams or other approved tools).

3.4. **Published contacts:** Only FBSU addresses may appear on the website, letterheads, forms, social media, advertisements and email signatures.

3.5. **Departments and roles:** Shared functions (admissions, registrar, HR, IT helpdesk) must use shared FBSU mailboxes managed by the IT Center, rather than individual accounts.

3.6. **Sensitive email:** Confidential and personal data sent by email must be encrypted in line with the Personal Data Encryption Policy (AD-095-1) and sent only to recipients who need it.

3.7. **Leavers:** On departure, an employee's FBSU mailbox is retained under the Documents Retention Policy (AD-80), and official correspondence is handed over to the line manager. Staff must not copy FBSU email to personal accounts.

3.8. **Exceptions:** Where an FBSU account is temporarily unavailable, the IT Center may approve a short, documented alternative. Any correspondence sent that way must be copied into the FBSU mailbox afterwards.

4. Work Data Storage

4.1. **Approved locations only:** FBSU data may be stored only in:

a. FBSU servers and databases managed by the IT Center.

b. The FBSU Microsoft 365 or Google Workspace tenant (OneDrive, SharePoint, Teams, Google Drive) under FBSU-managed accounts.

c. Other systems on the IT Center's approved list.

d. FBSU-owned devices that are encrypted and managed by the IT Center.

4.2. **Prohibited locations:** Storing, syncing or backing up FBSU data in any of the following is **prohibited**:

a. Personal cloud accounts: personal OneDrive, personal Google Drive, Dropbox, iCloud, WeTransfer, Mega and similar.

b. Any cloud tenant or account not owned by FBSU, including a previous employer's or another university's tenant.

c. Personal laptops, phones, tablets or home computers.

d. Personal USB drives or external disks.

e. Public code repositories (GitHub, GitLab) or personal repositories.

f. AI tools, except as allowed by the AI Acceptable Use Policy.

4.3. **Personal devices:** Personal devices may be used only to access FBSU services through the web or approved apps, without downloading or syncing files, and only if the device has a screen lock and current updates. The IT Center may require device management or block downloads on unmanaged devices.

4.4. **Sharing:** Files must be shared with named FBSU accounts. "Anyone with the link" sharing is not permitted for Confidential data. External sharing requires a documented business need and the approval of the data owner.

4.5. **Location of the tenant:** The IT Center records where each approved tenant and system stores its data. Confidential and personal data must be stored in the Kingdom, or under a transfer risk assessment approved by the IT Center in line with the Regulation on Personal Data Transfer outside the Kingdom and PDP Policy sections 8.21–8.23.

4.6. **Moving existing data:** Within 30 days of this policy taking effect, each user must move any FBSU data held in a prohibited location to an approved FBSU location, then delete it from the prohibited location, and confirm this to their line manager on the IT Center's form. The IT Center provides support and can arrange secure transfer.

4.7. **Vendors and contractors:** Vendors and programmers must keep FBSU data and code only in FBSU-provided environments, unless their contract allows otherwise and the IT Center has approved the arrangement.

5. Roles and Responsibilities

5.1. **Institutional Digital Transformation Committee (IDTC):** Recommends this policy for approval by the University Council; approves exceptions.

5.2. **IT Center:** Provides and manages FBSU email and storage; disables external forwarding; applies data loss prevention and sharing controls; keeps the approved systems list.

5.3. **IT Center (Data Protection):** Advises on the protection of personal data; approves any transfer risk assessment; handles data incidents, including notifications to SDAIA.

5.4. **Department heads and system owners:** Ensure that their teams use only FBSU email and storage; confirm compliance annually.

5.5. **All users:** Follow this policy; report misdirected email or data stored in the wrong place.

6. Monitoring, Compliance and Review

6.1. **Monitoring:** FBSU may monitor its email and storage systems, sharing settings and network traffic to enforce this policy, in line with applicable law. Monitoring shall be limited to what is necessary for this purpose, and users are informed of it through this policy.

6.2. **Incidents:** Official data found in a prohibited location, or sent through non-FBSU email, is a data incident. It must be reported to the IT Center-and handled under the Data Breach Response Plan (AA-405-F01).

6.3. **Compliance:** Breaching this policy may lead to loss of access and disciplinary action under FBSU regulations. Contractors and vendors may face contractual penalties.

6.4. **Review:** The IT Center and the IDTC review this policy annually, or sooner if national data protection or cybersecurity regulations change.

7. Policy Ownership and Approval

7.1. **Policy owner:** Information Technology Center.

7.2. **Reviewed by: Institutional Digital Transformation Committee (IDTC)**

7.3. **Approved by:** University Council.

7.4. **Date of approval:** 18-October-2026.

8. Related Documents

8.1. Personal Data Protection Law (PDPL) and its Implementing Regulations

8.2. Regulation on Personal Data Transfer outside the Kingdom

8.3. SDAIA General Data Sovereignty Policy

8.4. NDMO Data Management Standards

8.5. NCA Essential Cybersecurity Controls (ECC)

8.6. FBSU Personal Data Protection Policy (AD-095), especially section 8.17 (k) and (l), which already forbid personal data on mobile devices without IT Center approval and on employees' personal devices

8.7. Documents Retention Policy (AD-80)

8.8. Access Control Policy (AD-304)

8.9. Personal Data Encryption Policy (AD-095-1)

8.10. AI Acceptable Use Policy (IT-920)

8.11. Data Breach Response Plan (AA-405-F01)