Université Saint-Joseph de Beyrouth
جامعة القدّيس يوسف في بيروت

Access Management Policy

of Université Saint-Joseph de Beyrouth (USJ - Saint Joseph University of Beirut)

This policy was approved by the University Board during its 229th meeting on June 24, 2026

Objective	The access control policy specifies how the access is managed and who may have access to the information and information processing facilities and systems. It outlines the policies relating to granting privileges, controlling access and the review of user accounts and information systems.

Scope	This policy applies to all employees (including board members, deans and directors), students, teachers, suppliers, and other third parties accessing USJ's resources.

Roles	
CISO	The CISO is responsible for developing and updating this policy. The CISO must ensure that this policy is applied. The CISO must conduct yearly access review and ensure that the user matrix is up to date as requested by the HR and conduct periodic monitoring.
STI (IT Department)	They are responsible for applying this policy. They are responsible for applying the HR user matrix.
HR (Human Resources)	They are responsible for granting and revoking access. They must review and validate the user access matrix.
Staff	Users are responsible for submitting requests through the ticketing system.

Table of content

1. Principle of Least Privilege....4
2. Segregation of Duties....4
3. Role Based Access (RBAC)....4
4. Access Rights Review and Register....4
5. Account Provisioning....4
6. Access Right Changes....5
7. Account Termination....5
8. Access to Networks & Network Services....5
9. System and Application Access Control....5
10. Secure log-on procedures....6
11. Password Management....6

Details

1. Principle of Least Privilege

Access controls are allocated based on the business need and least privilege concept, which grants the user the strict minimum of access rights and permissions to the systems, services and resources to complete given tasks.

User accounts privileges on the workstations are managed through the Active Directory and Intune.

2. Segregation of Duties

Segregation of duties requires that critical tasks be divided among multiple individuals; no single person shall perform all steps of a process. This control prevents conflicts of interest and enables the detection of errors, fraud, or control failures.

In this regard, users must not be able to grant themselves administrative rights ; the CISO is responsible to monitor on a monthly basis the access rights including administrative privileges.

3. Role Based Access (RBAC)

Defining access rights within USJ is the responsibility of the CISO in coordination with the HR and IT department. The CISO shall ensure that accesses to the systems, network environment and PII are defined based on business requirements, job role, responsibilities and the access rights register.

Any alteration to the existing access must be submitted through a ticket and approved by the Director of the Institution/Faculty/Unit.

4. Access Rights Review and Register

All user access rights must be periodically reviewed and formally recorded to ensure they remain appropriate.

- All user accounts: reviewed at least annually
- Privileged accounts: reviewed at least twice yearly (with continuous monitoring)

Access rights must be registered and maintained in an access management system or controlled manual register.

Reviews must be documented for audit purposes.

5. Account Provisioning

User account access is created based on the least privilege principle mentioned previously taking into account that granting higher privileges must be temporary, justified and approved by the Director of the Institution/ Faculty/Unit

Employee onboarding should be conducted based on the following actions:

- Create a Microsoft 365 account;
- Prepare a new computer and install the default needed softwares (Microsoft Office, etc.);
- Enroll the device and the corporate mobile devices in the USJ Device Management tool;
- Encrypt the computer drives;
- Provide and setup an IP Phone extension;
- Enroll the employee physical access controls (HR responsability, like Keys, cards, etc.);
- Grant less privileges accesses either physical or logical;
- Enable access to folders according to the employee's role;
- Provision access to USJ systems and tools according to the employee's role.

Note: Personnel transferring from one area of responsibility to another shall have their access accounts modified to reflect their new job responsibilities and their previous accesses removed.

Provisioning of accounts and their privileges across USJ systems and applications must conform to the following requirements:

- Default account (e.g. Administrator, Guest, built-in accounts): System admin shall disable or rename these accounts on all devices (servers and workstations). Passwords must also be changed.
- Privileged account: is a type of administrative account having full access on either operating system or application level; accounts such as Administrators, super-administrators and, super-users are considered as privileged accounts.
- Allocation of access rights for similar accounts is given after getting an approval request by the CISO.
- Individual account: is a type of regular account that does not have any administrative access.
- System admin shall create the individual accounts based on the RBAC principle where each account has the appropriate privileges. The password must be changed regularly in reference to the Password policy. User accounts must be unique and traceable to the assigned user.
- External account (non USJ users): System admin will create an account when needed to complete specific tasks requested by USJ from the vendor or contractors (e.g. auditor, support). System admin must revoke access for external accounts once the specific task is completed. (using Privilege Access Management tool when feasible).

6. Access Right Changes

When a need for access right change arises, a request for access right change shall be created on the ticketing system and approved by the Director of the Institution/Faculty/Unit, this request should be received by the CISO for validation.

7. Account Termination

The access rights of an individual to information and assets associated with information processing facilities and services should be revoked or suspended during the de-registration phase via Active Directory and retire from the endpoint from USJ Device Management tool associated with the user whose account has been terminated.

User account access should be revoked on the day of termination. The account should be disabled; the data is backed up and archived or deleted if necessary.

An off-boarding form with the effective day of termination should be processed by HR based on the Employee Termination Policy. This policy should ensure that:

- The user access is revoked from all assets and systems such LDAP, IS, HR system, Access Control, online tools, phone, etc.
- All related devices are collected and reset before returning to stock (e.g. computer/mobile/Removable devices, etc.)

Note: Office365 data (emails and OneDrive files) can be recovered for up to 30 days after an account is terminated.

The CISO carries out a regular check, at least once per year, of the deregistered employees to ensure that the off-boarding process is well applied.

8. Access to Networks & Network Services

Network devices and network services should be protected from any unauthorized access using the Firewall controls such access lists. USJ Users are only allowed to access network and network services (e.g. VPN, Wireless network) based on their roles.

9. System and Application Access Control

USJ's systems and applications confidential and valuable information, thus access must be secured, controlled and restricted to authorized users only using secured procedures.

The CISO ensures that all new systems acquired will incorporate access controls.

10. Secure log-on procedures

The following procedures should be implemented to ensure secure and controlled access to systems and applications:

- Whenever technically possible, login to systems is authenticated by the Identity and Access Management (Active directory or Microsoft Entra ID);
- Whenever technically possible, configure two factor authentication for login to servers and systems;
- Enforce a rule against brute force log-on attempts;
- Enable the successful and unsuccessful attempts in the security logs to track all kind of log-on activities;
- Escalate any detected suspicious activity to the Infosec Administrator for investigation and remediation;
- Avoid displaying the password when entered during the logon process;
- Make sure to not share the password in clear text through emails;
- Enforce the logout principle after a period of inactivity.

11. Password Management

A password management solution should be enforced. Refer to Password Policy

Revision History			
Version	**Date**	**Reviewed and Approved by**	**Modifications**
01	March 2026	Developed by Patrick Hajj	
		Reviewed by Georges Nakhkeh and Fadi Chebli	
	May 2026	Reviewed and updated by Patrick Hajj	
	June 2026	Reviewed by Nadine Riachi Haddad	

Document Distribution			
Recipient	**Department**	**Date**	**Classification**
			Internal