

Clear Desk and Clear Screen Policy **of Université Saint-Joseph de Beyrouth** **(USJ - Saint Joseph University of Beirut)**

Objective

USJ is committed to safeguarding its information assets and ensuring compliance with all applicable laws and regulations regarding the handling of sensitive data.

All employees and any other parties with access to classified information must take appropriate measures to prevent unauthorized access. This includes ensuring that such information cannot be viewed by unauthorized individuals in any form, whether on paper, on removable media, or on a user's screen.

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 has to ensure that this policy is applied.

Employees, Teachers, Students

They are responsible for applying this policy.



Table of content

1. Clear Screen Policy	3
2. Clear Desk Policy.....	3
3. Other Forms of Display	5
4. Compliance and Enforcement	5

Details

This policy sets out the actions that should be taken to ensure that confidential and sensitive information remains secure, both during the working day and out of hours.

1. Clear Screen Policy

The following actions must be taken to ensure the security of information displayed on a computer or device screen:

- Screens must be locked when unattended, so that confidential and sensitive information is not displayed, and no access is available to restricted systems
- Screen locks must be protected by a password
- Care must be taken that screens are not sited such that the information displayed on them can be easily seen by unauthorised people
- Cameras or other recording devices (including mobile devices with a camera) must not be used in the vicinity of screens which may display confidential or sensitive information
- Avoid displaying and storing sensitive information on non-managed devices (phones, tablets, personal computers, etc), as they lack the security controls applied to USJ managed systems.

2. Clear Desk Policy

Creation and handling of materials containing confidential and sensitive information must conform to the following controls:

- Where possible, the printing of confidential and sensitive information must be avoided
- When classified information is printed, care must be taken that printouts are not accessible to unauthorised people
- Where possible, PIN-protected facilities (or similar) must be used when printing classified information
- When unattended, confidential and sensitive printed information must be locked away and appropriate control exercised over the key or other security mechanism
- Classified printed materials must not be left on desks (or other unsecured areas) outside of office hours
- It is strictly prohibited to display or attach confidential information (such as passwords, access codes, or sensitive data) on screens, desks, or any visible surfaces.
- Do not dispose of papers containing confidential or sensitive data in regular trash bins. All such documents must be shredded using approved shredders before disposal to prevent unauthorized access (e.g., dumpster diving).

Mobile devices and approved media that is used in an office environment must be subject to the following additional controls:

- Ensure laptops and mobile devices are secured when leaving your workspace
- Removable media, such as memory sticks and storage cards, that contain classified information must not be left unattended e.g. on desks
- Outside of working hours, removable media must be secured appropriately e.g. in a locked drawer or cabinet.

3. Other Forms of Display

In addition to the above, care must also be taken over confidential or sensitive information that may be displayed on other physical media, such as whiteboards, flip charts and sticky notes. These must be wiped or removed after use so that the classified information is no longer displayed.

Care must be taken when using collaboration tools such as Microsoft Teams, so that classified information is not visible in the background of a video call. If this is unavoidable, either a camera should not be used, or controls such as the use of standard background images or blurring of the background must be put in place.

4. Compliance and Enforcement

Non-compliance may result in disciplinary actions, this can include formal warnings or other measures as deemed appropriate by the university.

Revision History			
Version	Date	Reviewed and Approved by	Modifications
01	November 2025	Developed by Patrick Hajj	
	Janvier 2026	Reviewed by Nadine Riachi Haddad	

Document Distribution			
Recipient	Department	Date	Classification
			Internal