

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



Table of content

1. Objective
2. Aim
3. Scope
4. Responsibilities
 - 4.1 Chief Information Security Officer responsibilities
 - 4.2 IT Department responsibilities
 - 4.3 Vice-rector for administration responsibilities
 - 4.4 Data Protection Officer responsibilities
5. CCTV rules and regulations
6. CCTV Implementation
 - 6.1 Assessing the need for CCTV
 - 6.2 Acquisition and installation
 - 6.3 Management of CCTV monitoring
 - 6.4 Access requests
7. Policy implementation and enforcement

Annex – Access Form



1. OBJECTIVE

This CCTV Policy (hereinafter referred to as “**Policy**”) sets out the rules and procedures that must be followed when installing and dealing with Closed-Circuit Television (CCTV) to ensure the effective and lawful use of the CCTV systems within Saint Joseph University of Beirut (hereinafter referred to as “**University**”).

2. AIM

This Policy aims to ensure the privacy and security of individuals while providing a safe and secure environment.

3. SCOPE

This Policy applies to all CCTV systems owned, operated or controlled by the University and covers all locations where CCTV systems are installed.

4. RESPONSIBILITIES

4.1 Chief Information Security Officer responsibilities

The Chief Information Security Officer (CISO) is responsible for:

- Defining the required security control system;
- Following up the implementation of CCTV.

4.2 Information Technology Office responsibilities

The IT Office is consulted on the technical specs of the CCTV for compliance. It is responsible for:

- Connecting CCTV hardware to the University’s network;
- Managing the system user’s permission, storage and system network related configuration;
- Applying the security measures to provide segregation.

4.3 Vice-Rector for Administration responsibilities

The Vice-Rector for Administration (VRA) is responsible for:

- Overseeing the management of the CCTV systems in collaboration with campus administrators;
- Assessing the need for CCTV systems and the location of the cameras;
- Acquiring CCTV systems
- Installing, maintaining and repairing CCTV cameras through the Campus administrators.

4.4 Data Protection Officer responsibilities

The Data Protection Officer (DPO) is responsible for:

- Ensuring compliance with this Policy;
- Receiving camera access requests.

5. CCTV RULES AND REGULATIONS

CCTV has a legitimate role and objective to maintain a safe and secure environment for all its employees, staff, faculty, students and visitors and to reduce the risk of unauthorized access to premises and campuses and provide an accurate record of what happened when an incident occurred.

CCTV and its use are governed by the following policies and regulations:

- *Politique de conservation des données;*
- Data destruction policy;
- *Politique de protection des données dès la conception et par défaut;*
- Software Installation Policy;
- Anti-Fraud Policy;
- Personal Data Protection and Confidentiality Agreement;
- IT Hardware procurement Policy;
- Lebanese national legislation in force, law N°81/2018, relating to Electronic Transactions and Personal Data;
- General Data Protection Regulation N°2016/679.

6. CCTV IMPLEMENTATION

6.1 Assessing the need for CCTV

The acquisition of CCTV must be in the general interest of the University and the purchase order must be justified and duly validated by the VRA.

The University uses CCTV for the purposes of the management and security of the premises and campuses, monitoring health, safety and safeguarding of the employees, staff, faculty, students, and visitors.

USJ is the data controller for the use of CCTV.

6.2 Acquisition and installation

CCTV solutions should be assessed by the IT Department for compatibility and the CISO for compliance before being purchased and implemented. Hardware and software from known, verified and certified CCTV brands should be accepted and must ensure security and privacy in the design.

CCTV solution should be running on the University supported network switches and approved by the IT Department.

CCTV network should be an independent network and should never be mixed with administration network. VLAN solutions can be used to achieve this separation.


CCTV DVRs and monitors should be housed only in a dedicated and secured room, separate from the IT Department rooms with exclusive access to an IT authorized person, having the key of the room. Otherwise, no one has the right to access the dedicated room which must always be locked.

Cameras are not hidden from the view and sited appropriately in the area to be monitored, avoiding the recording of individuals outside the area for which a legitimate interest is claimed.

Cameras shall not be installed in non-public areas like faculty and staff offices, secretariat, meeting rooms, exam rooms, and any utility rooms (for example but not limited to: restrooms, kitchens, closed offices).

Images must be of sufficient quality for the purpose intended in this Policy.

It is strictly forbidden to listen to and record sounds, therefore, it is prohibited to connect the sound system of the cameras to the DVRs or any other device.



Appropriate privacy notices must be displayed in the areas that are subject to CCTV monitoring. The IT department must verify and test the system to technically validate the installation before final acceptance. Any camera or CCTV system (DVRs, monitors, etc.) already installed and which does not respect this procedure must be dismantled immediately.

6.3 Management of CCTV monitoring

Appropriate training should be provided to designated IT authorized personnel in the management and operations of the CCTV system, to allow them to carry out their roles and responsibilities effectively and lawfully.

CCTV images will be retained securely for a period of 6 months. This may vary in different circumstances and so retention period will be defined according to the situation or context in which a particular CCTV camera is operated. Once the retention period has expired, images must be securely deleted, if appropriate via an automatic process.

Access to CCTV cameras, live displays and recordings are protected and restricted to IT authorized personnel only, subject to DPO approval.

CCTV cameras and recording equipment must be tested on a planned basis to ensure that they are functioning correctly and that recorded images are of sufficient quality.

Recorded images must be protected in a way that takes account of the level of risk and sensitivity of the information contained – where appropriate, encryption techniques may be used to ensure confidentiality in situations such as the theft of the recording equipment. If cloud storage is used, due diligence must be carried out to ensure that the level of protection of the data is adequate.

6.4 Access requests

Any individual with a legitimate interest may submit an access request to obtain CCTV images. Such requests will be subject to a form submitted to the DPO (Annex – Request form), which will include all necessary checks to verify the lawful right to access and the identity of the requester. When approved, recorded images may be viewed live (subject to access controls) or a permanent record of the images may be provided.

Requests to disclose CCTV images must be approved in writing by DPO in all cases. Unauthorized disclosure of CCTV images (including publishing on the Internet and to the media) may result in disciplinary and judicial action being taken.

When appropriate, actions must be taken to obscure the identity of people and information that is not relevant to the request.

7. POLICY IMPLEMENTATION AND ENFORCEMENT

This Policy shall be implemented as of the date of its adoption by the University Board and may be amended by the University Board in accordance with the provisions of article 66 of the University Bylaws.

Annex - Request form

Requesting individual information:

Name:
Email address:
Phone number:.....
Faculty/Institute/Department:
Recording requested date:
Recording requested timeframe:

Reason for requesting recording:

.....
.....

Brief description of reason recording is needed:

.....
.....

Conditions:

- 1. Requests to review recordings from security cameras installed on the property of Saint Joseph University of Beirut must be approved by the Data Protection Officer. Completion of this Request form is only an application for request and does not constitute approval to view recordings. You will be notified in writing that your request has been either approved or denied. If approved, the Data Protection Officer will notify you on the method of access.
- 2. Any unauthorized use, reproduction, or distribution of the recordings is strictly prohibited.
- 3. Saint Joseph University of Beirut assumes no responsibility or liability for any use of the recordings in any way whatsoever.

By signing this form:

- I certify that all information provided is true and accurate to the best of my knowledge. Submission of false information could subject me to disciplinary action by Saint Joseph University of Beirut.
- I agree to abide by the terms and conditions set forth in this Request form and in the CCTV Policy.

Date:

Signature: