ATENEO CCTV POLICY

The Ateneo de Manila University ("Ateneo" or "University") operates systems of Closed Circuit Television (CCTV) cameras and related equipment within its premises in order to enhance campus safety and security for all members of its community.

This Policy establishes the rules that govern such systems. It is consistent with applicable University Privacy Policies and complies with all applicable laws and regulations, including the Data Privacy Act of 2012 (DPA) and its Implementing Rules and Regulations, National Privacy Commission (NPC) Circular No. 2024-02, Quezon City Ordinance No. SP-2695 (s. 2018), and Pasig City Ordinance No. 02 (s. 2014).

A. SCOPE OF POLICY

This policy applies to all CCTV systems owned and managed by the University at its Loyola Heights, Rockwell, Salcedo, and Ateneo School of Medicine and Public Health (ASMPH) campuses. It does not cover those that may be owned or maintained by Affiliated offices located within such campuses, or those in satellite offices located off-campus.

B. PURPOSE OF CCTV SYSTEMS

The University's CCTV systems are meant to perform a number of functions. They include:

1. Comply with government regulations and city ordinances
2. Secure properties and protect vital installations, including the perimeters of the campuses
3. Deter the occurrence of crime, inappropriate conduct, and violations of university policies
4. Maintain order and safety within campus premises
5. Track loss or theft of personal belongings
6. Protect vitally important interests of individuals
7. Monitor compliance with health standards
8. Provide necessary information for disciplinary, administrative, and criminal investigations
9. Aid in the verification processes of access control systems
10. Document incidents during emergency situations
11. Conduct vehicular and pedestrian counts essential for traffic and mobility studies

C. DEFINITION OF TERMS

For the purpose of this Policy, the following terms shall be defined as described hereunder:

1. "Access control systems" refers to a combination of software and security tools that control who can enter or exit a specific area.
2. "Affiliated offices" refers to offices or other entities not officially connected to the University but are located or operate within any one of its campuses.
3. *"CCTV Notice"* refers to a special kind of Privacy Notice that properly informs individuals of the existence and purpose of a CCTV system that is in operation. It must meet the requirements prescribed by NPC Circular 2024-02 (on CCTV Notices) and NPC Circular 2023-04 (on Privacy Notices).
4. "Closed circuit television" or "CCTV" refers to a closed-circuit television or camera surveillance system in a fixed or stationary location that can capture images of individuals or other information relating to individuals.
5. "Data breach" refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.
6. "Data subject" refers to an individual whose personal data is being processed.

CamScanner

7. "Organizational, technical, and physical security measures" refers to those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and against all other unlawful forms of processing.
8. "Personal data" refers to all types of personal information. It is the collective term used to mean personal information, sensitive personal information, and privileged information.
9. "Personal information" refers to any information, on its own or when combined with other information, from which the identity of an individual is apparent or can be reasonably and directly ascertained.
10. "Personal Information Controller" or "PIC" refers to a individual or organization that controls the processing of personal data, including one who instructs another individual or organization to process personal data on its behalf.
11. "Privacy Impact Assessment" or "PIA" refers to a process that evaluates and manages the impact on privacy of a particular program, project, process, measure, system or technology product.
12. "Privacy Notice" refers to a unilateral statement that contains essential information on one or more data processing activities.
13. "Privileged information" refers to any and all forms of data, which under the Rules of Court and other pertinent laws constitute privileged communication.
14. "Security incident" refers to an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity, and confidentiality of personal data. It includes incidents that would have resulted in a data breach, if not for safeguards that have been put in place.
15. "Sensitive Personal Information" refers to personal information:
    a. about an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
    b. about an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
    c. issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
    d. specifically established by an executive order or an act of Congress to be kept classified.

D. MANAGEMENT AND OPERATIONS

1. ***Campus Safety and Mobility Office (CSMO).*** It is responsible for overseeing the processing (e.g., collection, retention, use, sharing, etc.) of data, including personal data, carried out by the University's CCTV systems.
    a. It shall ensure that CCTV notices and, where appropriate, Privacy Notices are prominently displayed so that data subjects are properly informed of the existence of CCTV systems and their purpose.
    b. It shall implement contractual measures and/or adopt other mechanisms to ensure that appropriate safeguards are in place when the processing of CCTV records, wholly or in part, is outsourced to third parties (e.g., security agency contracted by the University).
    c. A PIA shall be undertaken regularly in coordination with the University Data Protection Office (UDPO) to evaluate the CCTV systems, or any part thereof, and check if they still serve their purpose and/or if they pose a risk much greater than the benefits they are expected to provide.

2. ***Security Area Commander.*** Subject to the instructions of the CSMO Director, the security agency contracted by the University shall facilitate the actual processing of data gathered

CamScanner

carried out by the University's CCTV systems. The agency shall be represented by the Security Area Commander whose duties shall include:

a. with prior clearance from the CSMO Director, identifying and assigning the CCTV system operators, or those personnel who will operate the CCTV systems. He is responsible for properly screening them and making sure they are adequately trained.
b. ensuring that only designated CCTV system operators and concerned security personnel have access to the CCTV systems in all CCTV monitoring rooms.
c. ensuring that all CCTV cameras and equipment are operational. All schedules for repairs and preventive maintenance shall be determined through consultation and coordination with CSMO.
d. ensuring that the CCTV systems are monitored by CCTV system operators at all times (i.e., seven days a week, twenty-four hours a day).
e. ensuring that all CCTV cameras are maintained within a secure network that may only be accessed by authorized personnel cleared by the CSMO Director.

3. ***CCTV system operators.*** They are responsible for the day-to-day operations and monitoring of the CCTV systems, including their protection from any: (1) unlawful interference or interception; (2) unauthorized access by copying, recording, or viewing; (3) accidental or unlawful destruction, alteration, and disclosure; and/or (4) other unlawful activities. They must also comply with all obligations prescribed by all applicable laws and administrative regulations including, but not limited to, the DPA, its implementing rules, and other relevant issuances of the NPC, such as:
    a. processing personal data strictly in accordance with the instructions of the CSMO Director
    b. implementing organizational, technical, and physical security measures
    c. cooperating and coordinating with the CSMO Director when addressing CCTV access requests

E. CCTV SYSTEM SPECIFICATIONS

Unless otherwise required by law or regulations, or subsequent updates to this Policy, the University's CCTV systems must meet the following minimum specifications:

1. The *Camera* must:
    a. have a minimum of 2-megapixel camera resolution
    b. be able to capture video footage at 0.5 lux illumination
    c. have auto-iris (either fixed or vari-focal) capabilities
    d. have Infrared LEDs capable of reaching a distance of at least 20 meters for clear recording at 0.1 lux (for areas where there is no continued sufficient lighting)
    e. have at least 70 degrees lens angle
    f. in the case of outdoor cameras, be vandal-proof or has IP 66 weatherproof casing

2. The *Video Recorder* must:
    a. have a minimum of four (4) camera input
    b. have a minimum of 720p video resolution
    c. have 30 frames per second (FPS) recording per camera
    d. have Hard Disk Drive/s that is/are capable of storing video recording for all cameras for at least one (1) month
    e. have Time Stamping feature
    f. have an interface for storage back-up

3. *Other components and/or specifications.* The *CCTV system* must have:
    a. a centralized power supply for the NVR and cameras
    b. POE (Power Over Ethernet) capability

CamScanner

c. appropriate Uninterruptible Power Supply (UPS) to provide standard and reasonable backup power to the video recorder and its cameras
d. standard Compression: H.264, MJPEG
e. Open Network Video Interface Forum (ONVIF)
f. network accessibility
g. smart phone and/or tablet support for off-site viewing

F. INSTALLATION

The installation of CCTV systems shall be subject to the following conditions:

1. Cameras must be installed at a secure location with a maximum area of coverage.

2. The video recorder must be mounted in a secure and concealed location to protect the video footage from theft and/or deliberate destruction.

3. CCTV cameras may be installed in the following areas of each campus, provided that their purpose or intended use is found in Section B of this Policy:
    a. campus gates, roads, sidewalks, pedestrian crossings, road intersections, pathways, driveways, parking areas, perimeter fence, and the Church of the Gesu
    b. open areas, sports facilities such as covered courts, football fields, baseball fields, tennis courts and swimming pools
    c. building entrances, lobbies, corridors, stairways, classrooms, reception areas, offices, areas of transaction and risk (such as tellers, cashiers, cash registrars, sales counters, or areas leading to the vault/safe), faculty rooms, libraries, auditoriums, theaters, chapels, laboratories, conference rooms, multi-purpose rooms, cafeterias, storage rooms, utility rooms, ring main unit (RMU), non-medical consultation rooms and common areas of residence halls.

4. CCTV cameras shall be prohibited in all areas with a heightened expectation of privacy, such as, but not limited to, restrooms, dorm rooms, lactation rooms, infirmary isolation rooms, and clinic consultation rooms.

5. CCTV Notices and, where appropriate, Privacy Notices shall be conspicuously installed within campus premises in all campus gates, road networks, common areas, building entrances and floor levels to indicate the presence of CCTV cameras and to provide information on the CCTV systems in place.

G. MONITORING OF THE CCTV SYSTEM

If, while monitoring the CCTV system, CCTV system operators have a reason to believe that a crime or a violation of a university policy has been committed, is being committed, or is about to be committed, they shall immediately inform the Area Commander who, in turn, shall confirm the report. Once a confirmation is made, the Area Commander shall notify the CSMO Director.

Once notified, the CSMO Director shall, in consultation with the Director of the University Legal and Compliance Office (ULCO), determine the appropriate course of action, including the need to contact the appropriate law enforcement agency and to provide the latter with access to pertinent CCTV records, subject to applicable laws and regulations.

H. STORAGE AND RETENTION OF CCTV RECORDS

Under the supervision of the CSMO, the storage and retention of CCTV records shall be subject to the following conditions:

CamScanner

1. *Secure storage.* CCTV records, and all related data and documents, shall be stored securely to ensure their confidentiality, integrity, and availability. In particular:
    a. Disk drive storage containing the video recordings shall be safely stored in racks located inside the CCTV monitoring rooms.
    b. Servers used as storage for CCTV records shall be securely stored inside the server room of the Office of the Vice President for Digital Information and Technology Services (OVPDITS).
    c. Access to the storage area shall be restricted to authorized personnel only.
    d. A password, set by CSMO, shall be required before authorized personnel can access CCTV records.
    e. An access log shall be maintained to document entries to the storage room.
    f. Access logs for CCTV records shall be regularly updated to ensure accurate record-keeping.

2. *Standard retention schedule.* The standard retention schedule for CCTV records is one (1) month from the date it is taken or captured. However, CCTV records may be retained for an extended period when required by applicable law or regulations, or there is a lawful order by a competent court or body, or when they hold investigative value, as determined by the University.

3. *Backup copy.* A backup of the CCTV records shall be maintained to ensure their availability, even in the event of a security incident or disaster, whether natural or man-made.

I. ACCESS TO CCTV RECORDS

Access to CCTV records shall be subject to the following conditions:

1. *Receiving Unit.* A CCTV access request shall be directed by the Requesting Party to the appropriate Receiving Unit:

Table A

REQUESTING PARTY	RECEIVING UNIT	DESIGNATED OFFICER
Employee of Ateneo (except those who are members of a school unit) or an Affiliated Office	CSMO Director	CSMO Director
Member of a school unit (i.e., employee or independent contractor)	School Unit	(see: Table B)
Student	School Unit	(see: Table B)
Law enforcement agency, fiscal/prosecutor, or court	CSMO Director [NOTE: The ULCO Director shall, at all times, be furnished with a copy of this type of request.]	CSMO Director
Visitor or parent of a student	School unit	(see: Table B)
Other interested parties	CSMO Director	CSMO Director

CamScanner

Table B

SCHOOL UNIT	DESIGNATED OFFICER
Grade School	Assistant Headmaster for Administration
Junior High School	Assistant Principal for Administration
Senior High School	Assistant Principal for Administration
Loyola Schools- Higher Education Under Graduate Student	Office of the Associate Dean for Student Affairs
Loyola Schools- Higher Education Graduate Student	Assistant Vice President for Graduate Education
ASMPH	Assistant to the Dean
Ateneo Graduate School of Business (AGSB, Rockwell Campus)	Assistant Dean for Admin and Student Services
Ateneo Law School	Assistant to the Dean for Administration
Ateneo School of Government	Academic Head
AGSB - CCE	Executive Director, Center for Continuing Education (CCE)

If in any of these cases, the Requesting Party does not want to refer the CCTV access request to the designated Receiving Unit due to a potential conflict of interest or some other valid reason, the request may be submitted directly to the CSMO Director: *Provided*, that if the CSMO Director determines that a proper endorsement is still necessary, the request will still be referred to the designated Receiving Unit: *Provided further*, that if the CSMO Director himself has a conflict of interest, the request shall be referred to the Vice President for Administration.

2. *Identity of the Requesting Party.* Before a CCTV access request is formalized, the Receiving Unit shall first verify the identity of the Requesting Party by asking said Requesting Party to present a valid government-issued ID. This applies even to former students or employees of the University. For current Ateneo students or employees, an Ateneo-issued ID may be presented as an alternative.

   If the Requesting Party is acting through an authorized representative, the identity of said representative shall also be verified. In addition, a proper authorization letter or document must also be presented.

3. *CCTV access request form.* Once the identity of the Requesting Party has been confirmed, the Receiving Unit shall formalize the request by asking the Requesting Party to accomplish a CCTV access request form. For Basic Education, the Endorsing Unit shall be the one to accomplish the form. The CSMO Director or Designated Officer, whichever is applicable, may delegate this task to another member of their office. A form that has been properly accomplished must contain the following information, as a minimum:
   a. Name of requesting school unit (if applicable)
   b. Name/s and Category of Data Subject or Third Party
   c. Type of Request (Viewing of footage or Security Report)
   d. Purpose/s of the request for access in line with the purpose/s of the CCTV system
   e. Specific date/s, approximate time, location, and any other important information regarding the subject of the request

   If the Receiving Unit determines that the Requesting Party has provided incomplete information or unsatisfactory proof of identity, it shall inform the latter within the prescribed processing time and request for the missing information and/or additional identification

CamScanner

5. *Conditions for Disclosure.* CCTV records may be disclosed or accessed under the following conditions:
    a. *Request by a Data Subject.* The request is made by a Data Subject (i.e., an individual whose image is in the CCTV record). If the CCTV record includes images of other individuals, disclosure may still be possible if the University and/or the Receiving Party has a legitimate interest in said disclosure, and it is not overridden by the rights of said other individuals (see: Section 12.f of the DPA). Should it involve Sensitive Personal Information of those other individuals, disclosure may still be made if: (1) it is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings; (2) if it is necessary for the establishment, exercise or defense of legal claims; or when it is to be provided to government or public authority (see: Section 13.f of the DPA).
    b. *Law Enforcement.* The request is from a law enforcement authority conducting a criminal investigation, pursuant to its constitutionally- or statutorily-mandated function: *Provided,* that the law enforcement authority must provide a written statement or affirmative declaration to establish the lawfulness of its request: *Provided further,* that the request adheres to existing standard operating procedures of the concerned law enforcement authority.
    c. *Court Orders.* The request is made through a lawful court order.
    d. *Administrative Investigations.* The access request is related to an administrative investigation: *Provided,* that the Requesting Party gives sufficient proof of an ongoing administrative investigation.
    e. *Media Requests.* The request is from a legitimate journalist or member of the press: *Provided,* that said request is based on a lawful ground that ensures respect for privacy rights: *Provided further,* that if the request involves identifiable individuals, the Requesting Party must be able to demonstrate that the CCTV records will not be used for entertainment purposes without the consent of all affected individuals.
    f. *Other Third-Party Requests.* The request is from other third parties. Each one shall be evaluated carefully to protect the privacy rights of all affected individuals. The requested information will only be released or disclosed if it is determined that the Requesting Party's needs outweigh those of the data subjects.

6. *Approval or Denial of Request.* The decision to approve or deny a CCTV access request shall be subject to the following conditions:
    a. The CSMO Director shall carefully evaluate the merits of each request, especially the declared purpose thereof. A request shall be approved if the CSMO Director determines that it is complete and satisfies the requirements of this Policy and the NPC Guidelines on the Use of Closed-Circuit Television Systems (NPC Circular No. 2024-02). Otherwise, the CSMO Director shall deny the request by sending a written notice to the Requesting Party within the prescribed processing time, stating the reason for the denial. For denied requests, requesting party may send an appeal letter to the Vice President for Administration
    b. *Access request via viewing.* If an access request (via viewing) is approved by the CSMO Director, the Requesting Party will be allowed to review the requested CCTV record. To ensure the confidentiality of the material, the Requesting Party will be required to sign an Undertaking. The Requesting Party is prohibited from capturing or recording the CCTV record during the viewing session. Only authorized CCTV personnel and, upon approval of the Requesting Party and the CSMO Director, the Designated Officer or another authorized school unit representative, shall be allowed to enter the CCTV monitoring room.
    c. *Access request via a copy of the CCTV record.* If an access request (via a CCTV record copy) is approved by the CSMO Director, the Requesting Party must provide a compatible storage device where the relevant CCTV record will be transferred or copied to. To avoid compromising the CCTV Systems in the event that the Requesting Party's storage device has malware, CSMO will send the copy to the

CamScanner

Requesting Party via email or some other online means. CSMO shall make sure to put a watermark on the video.

d. An access request may be denied based on following grounds:
   1.) incomplete information regarding the requested CCTV record
   2.) access request is frivolous or vexatious
   3.) purpose of request is contrary to law, morals, or public policy
   4.) request to obtain a copy is disproportional to the intended use
   5.) burden or expense of providing access is unreasonable or will involve a disproportionate effort on the part of the University
   6.) CCTV record has been deleted by the time the CSMO Director receives the request, in accordance with the standard retention schedule
   7.) sharing the CCTV record could put an ongoing criminal investigation at risk.

7. *Processing time*. Submitted CCTV access requests shall be processed within five (5) working days from receipt thereof by the Receiving Unit. Requests for copies of CCTV records shall be processed within fifteen (15) working days from receipt thereof. If a request is complex and/or involves multiple CCTV records, the processing time may be extended for fifteen (15) additional working days. In such a case, CSMO shall notify the Requesting Party in writing within the prescribed processing time, indicating the reason for the extension and, where applicable, the target date of release.

   For the purpose of this provision, a request is considered submitted once the Requesting Party fulfills the requirements outlined in Sections I.1 to I.3 of this Policy.

8. *Interpretation*. Any doubt as to whether access to CCTV records should be granted (partial or full) or denied shall be liberally interpreted in a manner that would uphold the rights and interests of the individual or individuals whose personal data is featured on said records.

9. *Effect of Access Request to Standard Retention Schedule*. When a request to view or obtain specific CCTV records is officially filed with CSMO, the latter shall preserve the relevant footage even if it means keeping the CCTV record beyond the standard retention schedule. The preservation of the CCTV record will remain in effect until the access request is fulfilled or abandoned.

10. *Abandoned request*. A request is deemed abandoned if the requesting party fails to fulfill or present the necessary requirements within thirty (30) days of notifying CSMO of its intention to access CCTV records.

J. POLICY REVIEW

This policy will be reviewed by the CSMO and OVPA in consultation with ULCO and UDPO. If necessary, it shall be revised before the start of every school year so as to incorporate any changes in applicable laws or regulations, or relevant University policies.

K. EFFECTIVITY

This policy will take effect one (1) month after approval by the President.

Approved by:

Roberto C Yap SJ
President
Date: 12 January 2026

CamScanner