



DATA PROTECTION OFFICE

Cebu Technological University (CTU) CCTV Privacy Policy

1. Purpose

This policy governs the use of Closed-Circuit Television (CCTV) systems at CTU, with the objective of:

- Ensuring the safety and security of students, faculty, staff, visitors, and University property.
- Deterring, detecting, and investigating unlawful acts (theft, vandalism, misconduct).
- Supporting administrative, disciplinary, and legal processes.
- Complying with the Data Privacy Act of 2012 (RA 10173), its Implementing Rules & Regulations (IRR), NPC Circular No. 2024-02 ("CCTV Systems"), and other relevant NPC issuances.

2. Scope

This policy applies to:

- All CCTV systems installed, operated, managed, or maintained by CTU across its campuses, including common areas, classrooms, laboratories, administrative offices, parking lots, etc.
- All personnel involved in procurement, installation, maintenance, monitoring, operation, access, storage, retention, and destruction of CCTV footage.
- All students, employees, contractors, visitors, and third parties whose images may be captured.

Excluded: CCTV systems used for purely personal, family, or household affairs, unless they capture images beyond private, non-commercial premises (per NPC Circular 2024-02).

3. Legal Basis & Principles

In line with NPC Circular No. 2024-02, CTU shall observe the following foundational data privacy principles:

Principle	Explanation / Application at CTU
Transparency	CTU will publicly display notices in conspicuous places (e.g., at building entrances, near CCTV coverage zones), stating that CCTV is in operation; what is being monitored; the purposes of CCTV; identity of the controller; and data subject rights.
Legitimate Purpose	CCTV systems will only be used for lawful, defined, campus-relevant objectives. Uses must conform to law, public policy, morals, and safety/security. Purpose(s) must be documented. Consent is not always required; CTU must choose a lawful basis under the Data Privacy Act (e.g., legitimate interest, legal obligation).





DATA PROTECTION OFFICE

Principle	Explanation / Application at CTU
Proportionality & Data Minimization	Systems must not intrude more than necessary. Camera placement, angles, zoom, and rotation must avoid capturing areas with heightened expectations of privacy. Use less intrusive means if available. Limit data collected to what is necessary.
Fairness & Lawfulness	Processing must be fair, non-discriminatory, and not oppressive; must comply with the Data Privacy Act, IRR, and NPC Circulars.
Accountability	CTU (as a Personal Information Controller, PIC) is responsible for demonstrating compliance: maintaining policies, reviewing practices, doing Privacy Impact Assessments (PIA) when required, auditing, and training.

4. Notice & Signage

- Notices must be readily visible and prominently displayed at all points of entry and other conspicuous areas in premises under CCTV coverage. These notices must clearly state the nature, purpose, extent, and scope of surveillance, the identity of the CTU as the controller, and the rights of data subjects.
- Signage should include details like camera coverage area, time of operation if not continuous, and whether audio is recorded (if applicable).

5. CCTV Policy & Operational Details

CTU shall maintain a detailed, written CCTV System Policy, which includes:

- Legitimate purposes and lawful bases for CCTV data processing.
- Operational details: procurement, installation, maintenance, camera location & orientation, devices' capabilities (zoom, night vision, rotation), metadata inclusion (timestamps, location).
- Responsibilities of authorized personnel: who monitors live feeds, who handles access, requests, and disclosure.
- Procedures for handling requests for access to footage (viewing, obtaining copies), including identity verification, specifying date/time/location, purpose, etc.
- Procedures and timeframes for handling complaints, inquiries, and personal data breaches or security incidents involving CCTV footage.
- Retention policy: duration, storage, and secure disposal or automatic deletion when no longer needed for the declared purpose. Retention should not exceed what is necessary.
- Security measures to protect footage and associated metadata (prevent unauthorized access, alteration, disclosure, destruction). Logging, audit trails, encryption, and physical security.
- Policy for regular review, audit, and revision of the CCTV policy and practices.





DATA PROTECTION OFFICE

6. Access, Disclosure & Requests

- Access by Data Subjects: Individuals may request to view or obtain copies of CCTV recordings in which they are captured. Requests must include sufficient details (date, time, location) and proof of identity.
- Third-Party / Law Enforcement Requests: CTU will require written, lawful requests or court/subpoena orders where applicable. Requests are evaluated carefully to balance security/law enforcement needs vs individual privacy rights.
- Denial of Request: Access may be denied on specific grounds, including:
 1. Incomplete request or lack of specificity.
 2. Request is frivolous, vexatious, or the burden is disproportionate.
 3. Purpose or manner of access conflicts with law, public policy, or morals.
 4. Footage has already been deleted per retention policy.
 5. Disclosure could jeopardize the ongoing investigation.
 6. Existence of disproportionality given declared purpose. SKY Law+1
- Timeframes for Response: Establish response timelines (e.g., within 7 working days for view-only requests; longer for copies, depending on complexity). If delayed, CTU must notify the requester and provide justification for the extension.
- Masking / Redaction: If footage is to be disclosed publicly (e.g., media), images of other persons not central to the request should be masked or obscured to protect their privacy.

7. Retention, Storage & Destruction

- Footage must be stored securely with appropriate metadata (timestamp, camera ID/location).
- The retention period should be explicitly documented, aligned with the legitimate purpose, and should not be longer than necessary. If there is a pending request or investigation, specific footage must be preserved beyond regular retention if needed.
- After the retention period lapses (and no legal or administrative reason to keep), data must be permanently and securely destroyed or irreversibly deleted.

8. Security and Safeguards

CTU must implement reasonable and appropriate safeguards, including:

- Access control measures: only authorized personnel may monitor live feeds or access stored footage.
- Physical security of recording equipment, storage devices, and control rooms.
- Encryption or secure storage methods.
- Audit logs recording who accessed footage, when, what was accessed, and what disclosures (if any).
- Regular maintenance, checking, and testing of CCTV hardware and software.





DATA PROTECTION OFFICE

- Privacy-by-Design and default features: ensure that the design and selection of CCTV systems consider privacy risks from the outset.

9. Privacy Impact Assessments (PIA) and Policy Review

- CTU should conduct PIAs:
 - When installing new CCTV systems or significantly altering existing ones (e.g., adding new camera functions like motion tracking or analytics).
 - Regularly thereafter, as part of compliance and risk assessment.
- The CCTV policy shall be reviewed and updated at least annually, or sooner if required by law, changes in technology, or operational needs. Audits to assess policy implementation, compliance, and effectiveness should also be performed.

10. Data Subject Rights

CTU affirms and will enable the following rights for individuals captured by CTU CCTV systems:

- Right to be Informed: via signage and policy disclosures.
- Right to Access: ability to view or obtain copies of relevant recordings, subject to verification and lawful grounds.
- Right to Rectification / Erasure: Where possible and lawful, errors or irrelevant footage may be requested to be corrected or erased, especially if it exceeds the necessary scope.
- Right to Object: to processing in certain circumstances, e.g., if overreaching, disproportionate.
- Right to Lodge Complaints: through CTU's internal grievance mechanism and/or the National Privacy Commission.

11. Accountability, Governance, and Roles

- Personal Information Controller (PIC): CTU holds responsibility for ensuring compliance with law and Circular 2024-02.
- Data Protection Officer (DPO): monitors policy implementation, responds to access/breach incidents, and ensures compliance with NPC guidelines.
- Authorized Personnel: Security Office and other designated staffers with clearly defined roles who manage live monitoring, handle requests, and maintain systems.
- Contracted Processors (PIPs): If any operations are outsourced (e.g., maintenance, storage, third-party monitoring), contractual agreements must ensure they also comply with NPC Circular, Data Privacy Act, uphold security, confidentiality, and the duty to assist the PIC.





DATA PROTECTION OFFICE

12. Exceptions & Heightened Privacy Areas

- CCTV shall not be installed in areas with a heightened expectation of privacy (e.g., restrooms, locker rooms, changing areas, private dormitories, private counselling or health clinics), except under extraordinary, lawful circumstances, and after stringent review.
- Audio recording is avoided unless necessary, and if used, must comply with legality and be disclosed explicitly.

13. Enforcement & Consequences

- Failure to comply with this policy and NPC Circular No. 2024-02 may result in administrative, civil, or criminal penalties under the Data Privacy Act and other applicable laws.
- CTU reserves the right to impose disciplinary actions on personnel who violate policy (unauthorized access, misuse, non-reporting).

14. Review & Effective Date

- This enhanced policy becomes effective March 21, 2025, aligning with the enforcement date of NPC Circular No. 2024-02 (August 27, 2024).
- Policy shall be reviewed at least annually, or sooner in response to:
 - Technological changes (e.g., new camera capabilities, AI/analytics),
 - Legal/regulatory updates,
 - Incidents of data breach or misuse,
 - Changes in campus infrastructure or campus security needs.

15. Contact Information

For questions, access requests, complaints, or other concerns:

Data Protection Officer (DPO)
Cebu Technological University
Main Campus, R. Palma St., Cebu City
Email: privacy@ctu.edu.ph
Phone: +639176508150

