Safety and Security Camera Acceptable Use Policy

Category: Administration and Governance  
Responsible Office: University Police  
Responsible Executive: Vice President for Finance and Administration  
Date Established: to be determined  
Date Last Updated: 03/05/2020

Summary

This policy provides guidance on the installation of video surveillance equipment and the handling, viewing, retention, dissemination, and destruction of video surveillance records.

Policy Statement

The University at Buffalo (UB, university) is committed to enhancing the quality of life of the campus community by integrating the best practices of safety and security with technology. A critical component of a comprehensive security plan is utilizing a security and safety camera system. Surveillance of public areas deters crime and assists in protecting the safety and property of the UB community.

The university uses security cameras and a single centralized video management system to enhance campus safety and physical facility security while respecting and preserving individual privacy. All security cameras placed on university property must be installed and operated in accordance with the Safety and Security Camera Procedures. Unapproved or nonconforming devices will be removed.

Information obtained from security cameras is considered university property and will be used for safety and security purposes and for law and university policy enforcement, including where appropriate, student, faculty, and staff judicial functions. Information obtained from security cameras is considered Category 2 - Private Data and must be handled with an appropriate level of security to protect against unauthorized access, alteration, or disclosure in accordance with the Protection of University Data Policy.

All appropriate measures must be taken to protect an individual’s right to privacy and secure university information through its creation, storage, transmission, use, and deletion.

Security Camera Installation

Security cameras may be installed to enhance the security and safety of people or property. Cameras are limited to uses that do not violate the reasonable expectation of privacy as defined by law. Where appropriate, cameras may be placed campus-wide, inside and outside buildings. All camera installations are subject to federal and state laws.

Security cameras will not be installed with the intent to conduct personnel investigations, such as those related but not limited to work place attendance, work quality, or academic conduct. However, the university may utilize security camera recordings captured during routine surveillance or in response to an incident in support of disciplinary proceedings against employees or students, or in a civil suit or other proceeding involving person(s) whose activities are shown on the recording and relate to the
proceeding. Information obtained in violation of this policy may not be used in a disciplinary proceeding against a university student or employee.

Security Camera Functions

Although the physical cameras may be identical, the security functions of these cameras fall into three main categories:

- **Property Protection** - The intent is to capture video and store it on a centralized video management system (VMS) so that if property is reported stolen or damaged, the video may show the perpetrator (e.g., unstaffed computer or science lab, parking lot)
- **Personal Safety** - The intent is to capture video and store it on a centralized VMS so that if a person is assaulted, the video may show the perpetrator (e.g., public lounge, walkway, parking lot)
- **Extended Responsibility** - The intent is to have the live video stream in one area monitored by a staff member in close proximity and to store the video on a centralized VMS (e.g., food service area or testing center with multiple rooms or stations and limited staff members acting as a manager or proctor)

Placement of Security Cameras

The locations where security cameras are installed may be restricted access sites (e.g., departmental computer lab), however, these locations are not places where a person has a reasonable expectation of privacy. Cameras will be located to maximize personal privacy and audio will not be recorded.

Security camera positions and views of residential housing will be limited. The view of a residential housing facility must not violate the standard of a reasonable expectation of privacy.

Monitoring by security cameras is prohibited in the following locations:

- Student living spaces in university residence halls and apartments
- Bathrooms
- Locker rooms

All video camera installations must be visible. The installation of “dummy” or placebo cameras that do not operate is prohibited.

Access and Monitoring of Security Cameras

All university security camera recording or monitoring of activities of individuals or groups will be conducted in a manner that is:

- Consistent with university policies and state and federal laws
- Professional, ethical, and legal
  - Personnel with access to university security cameras must be trained in the effective, legal, and ethical use of monitoring equipment
- Not based on the subjects’ personal characteristics including age, color, disability, gender, national origin, race, religion, sexual orientation, or other protected characteristics
University security cameras are not monitored continuously under normal operating conditions but may be monitored for legitimate safety and security purposes that include, but are not limited to the following: high risk areas, restricted access areas or locations, in response to an alarm, special events, and specific investigations authorized by the Chief of Police or designee.

For property protection, personal safety, and extended responsibility security cameras, access to live video or recorded video is limited to authorized personnel of the department which installed the cameras, University Police, and other persons authorized by the Chief of Police or designee.

Exporting, copying, duplicating, or retransmission of live or recorded video is limited to persons within University Police as authorized by the Chief of Police.

A record log will be maintained by the Vice President and Chief Information Officer (CIO) of all instances of access to, and use of, recorded material. Data will be kept for one year.

Nothing in this section is intended to limit the authority of University Police in law enforcement activities.

**Funding**

Security cameras must be purchased with State funds. Research Foundation and UB Foundation funds may not be used to purchase security cameras.

**Appropriate Use and Confidentiality**

Video management system users are prohibited from using or disseminating information acquired from university security cameras, except for official purposes. All information or observations made in the use of security cameras is considered confidential and can only be used for official university and law enforcement purposes.

**Background**

The university uses security cameras and a centralized video management system to:

- Enhance the safety of individuals and assets
- Support the university’s ability to prepare for and respond to emergencies
- Improve operational efficiencies and effectiveness

**Applicability**

Unless explicitly exempted, this policy applies to all personnel, departments, colleges, campus organizations, subsidiaries, tenants, and public/private partnerships with the university for the installation and use of security cameras and their video monitoring and recording systems on campus and in any university-owned or leased spaces.
This policy does not apply to:

- Security cameras used inside University Police headquarters and sub-stations
- Mobile or hidden video equipment used in criminal investigations conducted by University Police
- Covert video equipment used for non-criminal investigations of specific instances which may be a significant risk to public safety, security, and property as authorized by the Chief of Police or designee
  - The use of such cameras is subject to applicable state and federal laws as well as University Police internal policies and procedures
- Automated teller machines (ATMs), which may utilize cameras
- Cameras used for academic purposes
  - Cameras used for research are governed by policies involving human subjects
  - May not be used as a security camera or in another manner with the intent of circumventing this policy
- Webcams for general use by university personnel (e.g., webcams installed on individual workstations, laptops, tablets, or cellular telephones) used for legitimate business purposes (e.g., video conferences)
  - May not be used as a security camera or in another manner with the intent of circumventing this policy
- Use of video equipment to record public performances or events, sporting events, interviews, or other use for broadcast or educational purposes (e.g., videotaping athletic events for post-game review, videotaping concerts, plays, and lectures, or videotaped interviews)
  - May not be used as a security camera or in another manner with the intent of circumventing this policy

Definitions

Category 1 – Restricted Data

Protection of the data is required by law or regulation. The loss of confidentiality, integrity, or availability of the data or system could have a significant adverse impact on our mission, safety, finances, or reputation.

Restricted data includes the definition of private information in the New York State (NYS) Security and Breach Notification Act as a foundation: bank account, credit card, and debit card numbers; social security numbers; state-issued driver license numbers; and state-issued non-driver identification numbers. To this list, university policy adds protected health information (PHI), computer passwords, other computer access protection data, and passport numbers.

Category 1 – Restricted Data are exempt from disclosure or release under the NYS Freedom of Information Law (FOIL). The NYS Information Security Breach and Notification Act requires the university to disclose any breach of the data to New York residents. (State entities must also notify non-residents; see the NYS Information Security Policy.)

Individuals who access, process, store, or in any other way handle Category 1 – Restricted Data must implement controls and security measures as required by relevant laws, regulations, and university policy. In instances where laws and/or regulations conflict with university policy, the more restrictive policy, law, or regulation governs.

Category 2 – Private Data

Includes university data not identified as Category 1 – Restricted Data, and data protected by state and federal regulations. This includes Family Educational Rights and Privacy Act (FERPA)-
protected student records and electronic records that are specifically exempt from disclosure by the NYS FOIL.

Category 2 – Private Data must be protected to ensure that they are not disclosed in a FOIL request. Private data must be protected in order to ensure that they are only disclosed as required by law, including FOIL. Decisions about disclosure must be made by the Records Management Officer.

The National Institute Standards and Technology (NIST) Special Publication 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations maps to the Category 2 – Private Data risk classification.

**Reasonable Expectation of Privacy**

The reasonable expectation of privacy is an element of privacy law that determines in which places and in which activities a person has a legal right to privacy. Sometimes referred to as the "right to be left alone," a person's reasonable expectation of privacy means that someone who unreasonably and seriously compromises another's interest in keeping their affairs from being known can be held liable for that exposure or intrusion.

**Security Camera**

A device that records images and which is used to detect or prevent crime.

**Security Camera Oversight Committee (SCOC)**

Operational committee established by the Vice President for Finance and Administration to oversee implementation of this policy. The SCOC is comprised of the following members:

- Chief of Police, chair of the SCOC
- Vice President and Chief Information Officer or designee
- Vice President for Student Life or designee
- Associate Vice President for Human Resources
- Associate Vice President for University Facilities

**Responsibility**

**University Police**

- Approve department and unit requests to purchase and install security cameras.
- Select, coordinate, operate, manage, and monitor all campus security cameras and video management systems.
- Oversee the installation, support, maintenance, replacement, and decommissioning of all approved security camera systems.
- Provide advice to departments on appropriate applications of surveillance technologies.
- Provide technical assistance to departments preparing proposals for the purchase and installation of security camera systems.
- Review proposals and recommendations for camera installations and specific camera locations to determine that the perimeter of view of fixed location cameras conforms to this policy.
- Assess new camera locations and conduct an evaluation of existing camera locations and incidents as necessary.
- Test cameras and coordinate maintenance.
- Review complaints regarding utilization of surveillance camera systems.
- Review requests to release records obtained through security camera surveillance.
  - Seek consultation and advice from university legal counsel and other departments, as appropriate, prior to the release of any records.
o Direct Freedom of Information Law (FOIL) requests to the Records Management Officer.

- Monitor developments in the law, security industry practices, and technology so that camera surveillance is consistent with best practices and complies with federal and state laws.

Departments, Units
- Request approval to install video surveillance equipment from their vice president, dean, or department head.

Vice Presidents, Deans, Department Heads
- Review and approve, as appropriate, requests:
  o To purchase and install security cameras within their area of responsibility
  o For user access to the VMS to monitor and review video from departmental cameras
  o To export and save video

Vice President and Chief Information Officer
- Manage and maintain the:
  o Single centralized VMS
  o Campus data network infrastructure over which the security cameras will communicate with the VMS log of all instances of access to, and use of, recorded material

Video Management System (VMS) User
- Complete training in the technical, legal, and ethical parameters of appropriate security camera use.
- Operate security cameras.
- Watch both live and recorded video surveillance footage.
- Report incidents or suspicious behavior.
- Contact authorities when necessary.

Security Camera Oversight Committee (SCOC)
- Review and approve, as appropriate, requested exceptions to this policy.
- Review appeals of decisions made by the Chief of Police regarding complaints of surveillance camera systems.

Contact Information

<table>
<thead>
<tr>
<th>Contact</th>
<th>Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daryl Kempf</td>
<td>716-645-8938</td>
<td><a href="mailto:dlkempf@buffalo.edu">dlkempf@buffalo.edu</a></td>
</tr>
</tbody>
</table>
Related Information

University Links

Computing and Network Use Policy
http://www.buffalo.edu/administrative-services/policy1/ub-policy-lib/computer-network-use.html

Protection of University Data Policy

Safety and Security Camera Procedures (link to be added when published online)

Video Security Camera Service
http://www.buffalo.edu/ubit/information-for-it-staff/video-security-camera.html

Forms
Request a New Network Connection
Video Surveillance – New Camera Setup

Related Links
What is Invasion of Privacy?

Presidential Approval

__________________________________
Satish K. Tripathi, President

______________________________
Date
Safety and Security Camera Procedures

Compliance
Departments requesting security cameras must comply with the Safety and Security Camera Acceptable Use Policy and these Safety and Security Camera Procedures.

1. Procedures

1.1 Purchase and Installation
All personnel, departments, colleges, campus organizations, subsidiaries, tenants, and public/private partnerships with the University at Buffalo (UB) that wish to install video surveillance equipment on campus or in any university-owned or leased spaces must submit a written request to their vice president, dean, or department head describing the proposed location of surveillance devices, justifying the proposed installation, and identifying the funding source(s) for purchase and ongoing maintenance of cameras and related software and hardware licenses.

Security cameras must be purchased with State funds. Research Foundation and UB Foundation funds may not be used to purchase security cameras.

Approvals
- The vice president, dean, department head, or designee will review and approve the request, as appropriate, then forward to the Chief of Police.
- The Chief of Police or designee will review and approve or deny all requests for security camera equipment.

University Police approval is required to purchase security cameras to be installed on university property. UB Procurement Services will not accept, approve, or process any order for security cameras or video management systems without the approval of University Police.

University at Buffalo Police Department (UBPD) will oversee the installation, support, maintenance, replacement, and decommissioning of all approved security camera systems with the assistance of the Vice President and Chief Information Officer, University Facilities, and external vendors as appropriate.

1.2 Access and Training
Access to the video management system (VMS) to monitor and review video from departmental cameras will be granted to a limited number of staff members (VMS Users) as designated by the vice president, dean, or department head based on a business case need.

All access to the VMS must be approved by the Chief of Police or designee.

All personnel with access to the VMS (VMS Users) must be trained in the technical, legal, and ethical parameters of appropriate camera use.

VMS Users must provide written acknowledgement that they have received and understand the contents of the:

- VMS training
- Safety and Security Camera Acceptable Use Policy and these Procedures
1.3 Operation
Video surveillance will be conducted in a manner consistent with all existing university policies.

VMS Users will monitor based on suspicious behavior, not individual characteristics.

VMS Users will not view private rooms or areas through windows.

All VMS Users and supervisors involved in video surveillance will perform their duties in accordance with the Safety and Security Camera Policy and these Procedures.

Individual requests to export and save video must be submitted, in writing, to their appropriate vice president, dean, or department head describing the reason and justification for the video export request.

- The vice president, dean, department head, or designee will review the request and recommend it to the Chief of Police, if appropriate.
- The Chief of Police or designee will review and approve or deny all requests to export and save video.

1.4 Storage, Retention of Recordings, and Access Logs
Surveillance recordings must not be altered. Access to the VMS will be configured to prevent VMS Users from tampering with recorded information. Exporting, copying, duplicating or retransmission of live or recorded video will be limited to persons within UBPD as authorized by the Chief of Police.

Video recordings and surveillance records will not be exported or stored by individual departments.

All surveillance video and records will be stored in a secure, centralized university video management system for a minimum thirty (30) days and will then promptly be erased or written over, unless exported and retained as part of a criminal investigation or court proceedings (criminal or civil), or other bona fide use as approved by the Chief of Police or designee.

Requests to retain video from specific security cameras for periods longer than thirty (30) days must be approved by the Chief of Police or designee.

All VMS server logs will be stored in a secure, centralized university video management system for a minimum of one year and will then promptly be erased or written over, unless exported and retained as part of a criminal investigation or court proceedings (criminal or civil), or other bona fide use as approved by the Chief of Police or designee.

Individual departments will not be allowed to export or store video surveillance recordings.

1.5 Testing and Maintenance of Security Cameras
UBPD or their designee will be responsible for the testing and coordination of the support and maintenance of all security cameras that are part of the university central VMS.

University Police will be responsible for funding the maintenance, repair and replacement of:

- Cameras associated with the Campus Blue Light Phone System
- Non-departmental cameras associated with building perimeters and exteriors

Individual departments that request cameras to be added to the central VMS that cover interior or exterior departmental spaces must provide the necessary funding for the maintenance, repair, and replacement of those cameras.

1.6 Testing and Maintenance of the Video Management System
The Vice President Chief Information Officer will be responsible for the installation, support, maintenance, replacement, and decommissioning of hardware and software components that comprise the university central VMS with the assistance of the following university groups and external resources as required:

- Procurement Services
- Procuring department
- External vendors