SECURITY CAMERAS

POLICY NUMBER: ADM-SECURCAMS
POLICY TYPE: ADMINISTRATIVE
RESPONSIBLE OFFICIAL TITLE: CHIEF INFORMATION OFFICER
RESPONSIBLE OFFICE: OFFICE OF INFORMATION TECHNOLOGY
EFFECTIVE DATE: UPON PRESIDENTIAL APPROVAL –
NEXT REVIEW DATE: PRESIDENTIAL APPROVAL PLUS FOUR (4) YEARS –
SUPERSEDES POLICY DATED: N/A – NEW POLICY
BOARD OF REGENTS REPORTING (CHECK ONE):
☐ PRESIDENTIAL RECOMMENDATION (CONSENT AGENDA/VOTING ITEM)
☒ PRESIDENTIAL REPORT (INFORMATION ONLY)

I. POLICY STATEMENT

This policy provides guidelines for the use of security cameras on property owned and/or utilized by Northern Kentucky University (NKU) in a way that enhances safety and security while respecting the privacy of members of the University community.

The primary purpose of cameras in public areas is to deter crime and enhance the safety of the University community and University property. Cameras are used to record video for use by law enforcement and other University officials charged with investigating alleged violations of law or University policy and in furtherance of legitimate safety initiatives.

This policy is adopted to formalize procedures for the installation of security equipment and the handling, viewing, retention, dissemination, and destruction of surveillance records.

The existence of this policy does not imply or guarantee that security cameras will be monitored in real time continuously or otherwise.

II. ENTITIES AFFECTED

This policy applies to all Northern Kentucky University properties. For leased space, lessees are exempt from this policy if they have their own network. If they are using NKU's network, they are subject to this policy. The determination of whether a facility leased by the University will be subject to this policy will be made by the Chief of Police.

This policy applies to all faculty and staff employed by, and to all schools and departments within, the University. This policy shall not apply to:

- use of cameras for reasons unrelated to general recording of public spaces for broad safety and security goals
- remote monitoring of facilities construction and progress
- videotaping of athletic events for post-game reviews
- the use of cameras in connection with human subject and animal research
- the use of cameras in certain laboratories to ensure safe research practices
- the use of cameras for legitimate educational purposes

- cameras used by law enforcement in covert operations in conjunction with a criminal investigation
- mobile cameras used in, on, or about law enforcement or parking services vehicles
- body-worn or otherwise portable cameras used during the course of investigations or normal law enforcement functions
- parking enforcement cameras.

III. AUTHORITY

Responsibility for oversight of installation, maintenance, and utilization of security cameras and associated policies, standards, and procedures is delegated by the President of the University to the Chief Information Officer, University Legal Counsel, and the Chief of Police. This responsibility includes:

1. creation, maintenance, and review of a campus strategy for the procurement, deployment, and use of security cameras, including this and related policies;
2. designation of the standard campus security camera system or service;
3. authorizing the placement of all security cameras;
4. authorizing the purchase of any new security camera systems;
5. reviewing existing security camera systems and installations and identifying modifications required to bring them into compliance with this policy;
6. authorizing the decommission of campus security cameras;
7. creating and approving campus standards for security cameras and their use; and
8. creating and approving procedures for the use of security cameras.

IV. DEFINITIONS

As used within and for the purposes of this policy, the terms below are defined as follows.

Chief of Police: The head of the University Police Department in the Division of Student Affairs, or designee.

Private areas: Areas in which a person has a reasonable expectation of privacy, including, but not limited to, non-common areas of residence halls, residence hall corridors, bathrooms, shower areas, locker and changing rooms, and other areas where a reasonable person might change clothes. Additionally, areas designed for the personal comfort of University employees or the safeguarding of their possessions, such as faculty and staff offices, University Special Collections and University Archives in Steely Library, lounges and locker rooms, and areas dedicated to medical, physical, or mental therapy or treatment shall be considered private areas for the purpose of this policy.

Public areas: Areas made available for use by the public, including, but not limited to, campus grounds, parking areas, building exteriors, loading docks, areas of ingress and egress, classrooms, lecture halls, study rooms, lobbies, theaters, libraries, dining halls, gymnasiums, recreation areas, and retail establishments. Areas of the University in which persons would not have a reasonable expectation of privacy, but to which access is restricted to certain University employees, such as storage areas, shall also be considered public areas for the purpose of this policy.

Security camera: A camera used for monitoring or recording public areas for the purposes of enhancing public safety, discouraging theft and other criminal activities, and investigating incidents.

Security (or surveillance) camera monitoring: The real-time review or watching of security camera feeds.

Security camera recording: A digital or analog recording of the feed from a security camera.

Security camera viewing: The reviewing or watching of historical security camera feeds.

Security camera system: Any electronic service, software, or hardware directly supporting or deploying a security camera.

V. RESPONSIBILITIES

All university personnel involved in the installation, maintenance or monitoring of security cameras: (a) will be instructed in the technical, legal and ethical parameters of appropriate camera use; and (b) will receive a copy of this policy and provide a written acknowledgment that they have read and understand its contents.

Security Camera Placement

1. University Police shall coordinate oversight of temporary or permanent security cameras on campus. Schools, departments, and offices desiring the installation and use of security cameras shall submit a request for such installation to University Police. All installations must be approved by the area Vice President, Chief Information Officer, Legal Counsel, and the Chief of Police.
2. University schools, departments, and offices presently utilizing security cameras shall promptly advise the University Police Department, which will review the location and utilization of the security cameras and identify actions necessary to bring such usage into conformance with this policy.
3. Consistent with the requirements of state law (KRS § 526.020) security cameras utilized by the University will not record or monitor sound.
4. Use of security cameras shall be limited to public areas. Video surveillance shall be not conducted in private areas of the campus unless specifically authorized by the Chief of Police pursuant to a criminal investigation.
5. Where security cameras are permitted in private areas, they will, to the maximum extent possible, be used narrowly to protect persons, money, real or personal property, documents, supplies, equipment, or pharmaceuticals from theft, destruction, or tampering.
6. Inoperative, placebo, or “dummy” security cameras shall NEVER be installed or utilized, as they may lead to a false sense of security that someone is monitoring an operational camera.

Security Camera Monitoring and Review

1. The University Police may monitor and review security camera feeds and recordings as needed to support investigations and to enhance public safety. It is not intended or expected that security cameras will be routinely monitored in real time.
2. With the prior approval of the Chief of Police, other University personnel may monitor and review live security camera feeds and recordings for purposes of public safety or as the legitimate and efficient discharge of their responsibilities requires.

3. Monitoring individuals without cause, based on characteristics of race, gender, ethnicity, sexual orientation, disability, or other protected classification is prohibited.
4. Seeking out and continuously viewing people becoming intimate in public areas is prohibited.

VI. PROCEDURES

Use of Recordings

Security camera recordings, with the approval of the Chief of Police, shall be used for the purposes of enhancing public safety, discouraging theft and other criminal activities, and investigating incidents (including the release of recordings by University Police to external law enforcement agencies). Recordings from security cameras whose primary function is not security (such as classroom lecture capture) may be used for security purposes with the authorization of the Chief of Police.

The use of security cameras and/or recordings for any purpose not detailed within this policy is prohibited.

Records of access to and release of security camera recordings must be sufficient so as to demonstrate compliance with this policy.

Protection and Retention of Security Camera Recordings

Video footage will be stored on servers accorded appropriate computer security with access by authorized personnel only.

Northern Kentucky University will retain recordings from the Enterprise Camera Systems for 30 days. This retention period may be extended at the direction of University Legal Counsel or the Chief of Police or as required by law.

Release of Recorded Material

Requests for release of recorded material must be approved by the Chief of Police and University Legal Counsel. Requests for release of recorded material set forth in subpoenas or other legal documents compelling disclosure should be submitted to University Legal Counsel.

VII. COMPLIANCE

It shall be the responsibility of the Chief of Police to see that records related to the use of security cameras and recordings from security cameras are sufficient to demonstrate compliance with this policy. Before procuring security camera systems, units will need to ensure compatibility with the system identified as the campus standard by the Chief of Police.

The Chief Information Officer, and University Legal Counsel, in conjunction with the Chief of Police, may review the procurement, deployment, and utilization of security cameras at the University, whenever and as frequently as they deem necessary. A finding that a school, department, or office has failed to comply with the requirements of this policy may result in the loss of its privilege to support, maintain, or deploy security cameras and may result in other remedial action.

VIII. EXCEPTIONS

Uses of security cameras beyond those described in this policy shall be governed by applicable University policies and procedures. Persons having questions about the use of monitoring security cameras not subject to this policy should direct those questions to the Chief of Police or University Legal Counsel.

IX. REFERENCES AND RELATED MATERIALS

REFERENCES & FORMS

Kentucky Revised Statutes § 526.020, § 532.060, § 534.030: Recording or obtaining private communications in violation of Kentucky's eavesdropping law, as well as sharing images in violation of the state's video voyeurism law, are both considered felonies and are subject to a $5,000 fine and a maximum of five years imprisonment.

Kentucky Revised Statutes § 532.090, § 534.040: Infractions against Kentucky's hidden camera laws and sharing content intercepted by eavesdropping are considered misdemeanor offenses subject to a $500 fine and a maximum of one year in jail.

RELATED POLICIES

- Acceptable Use
- Code of Student Rights and Responsibilities

REVISION HISTORY

REVISION TYPE	MONTH/YEAR APPROVED
New Policy	

SECURITY CAMERAS

PRESIDENTIAL APPROVAL

PRESIDENT

Signature A. K. Vaidya Date 11/18/2020

Ashish K. Vaidya

BOARD OF REGENTS APPROVAL

BOARD OF REGENTS (IF FORWARDED BY PRESIDENT)

☒ This policy was forwarded to the Board of Regents on the ***Presidential Report (information only)***.
Date of Board of Regents meeting at which this policy was reported: 1 / 20 / 21.

☐ This policy was forwarded to the Board of Regents as a ***Presidential Recommendation (consent agenda/voting item)***.

- ☐ The Board of Regents approved this policy on _____/_____/_____.
  (Attach a copy of Board of Regents meeting minutes showing approval of policy.)
- ☐ The Board of Regents rejected this policy on _____/_____/_____.
  (Attach a copy of Board of Regents meeting minutes showing rejection of policy.)

VICE PRESIDENT AND CHIEF STRATEGY OFFICER

Signature Bonita Brown Date 02/10/21

Bonita J. Brown