I - SCOPE
This policy applies to all faculty and staff employed by, and to all schools and departments within the University of Maine System (UMS). Campuses of the University of Maine System (UMS) may utilize video technology to promote public safety, to protect personal and institutional property, and to support general crime prevention efforts. At the same time, each campus must respect the right to privacy of the entire campus community while providing a safe and secure environment. This policy shall not apply to use of cameras for reasons unrelated to surveillance activity. Also, authority for and use of police procedures will not be compromised by this policy.

Additionally, in cases where a facility is leased by a University, whether as lessor or lessee, the determination as to whether said facility will be subject to this policy will be made on a case-by-case basis by the President or his/her designee. Terms of the pertinent lease agreement, along with location and attributes of the facility are factors that would need to be evaluated.

Exceptions: A) This policy does not apply to video technology that is utilized for academic purposes. Such technology that is used for research activity is governed by other policies related to human subjects and is therefore excluded from this policy. B) Exceptional circumstances include the use of video surveillance technology by recognized law enforcement officials for covert surveillance purposes. Covert surveillance by law enforcement is governed by the U.S. Constitution; Maine State Law; and any associated policies established at the campus level.

II - Purpose and Utilization
The purpose of this policy is to provide guidelines for the use of security cameras on property owned and/or utilized by the UMS. The use of security cameras or other video surveillance technology must comply with this policy and focus on the enhancement of personal or property security. Such technology will be limited to locations and utilization in a manner that does not infringe on the reasonable expectation of privacy as defined by law, whether inside or outside of buildings.

Video surveillance must fall into one or more of three main categories:

1) Property Protection – the primary intent is to secure property and capture imaged media related to theft or damage. Such media may be stored on a remote device for later use to identify responsible individuals or for other appropriate purposes.

Examples of use include:
- Unstaffed computer laboratory
- Unstaffed science laboratory
- Parking area

2) Personal Protection – the primary intent is to capture imaged media related to an incident, then stored on a remote device to be utilized during the resolution of the incident.

Examples of use include:
- Public walkway
- Parking area
3) Extended Responsibility (Critical Understaffed Areas)– the primary intent is the monitoring of a live image stream from an area of close proximity by an appropriately trained university employee. The media may or may not be recorded. An example of use includes:
- Computer laboratory with multiple rooms and only one staff member

With the exception of Extended Responsibility situations, video surveillance technology is not monitored continuously under normal operating conditions. **Continuous monitoring** is allowed for legitimate safety and security purposes with prior and/or written approval (see Section III-Approval Process).

Examples of continuous use include:
- High risk area
- Restricted access area
- Residence Halls
- Specific event
- Specific authorized investigation

### III - Approval Process

Each campus will develop an appropriate review and approval process, such as the establishment of a Governance Team, for the addition, removal, continuous monitoring or relocation of video surveillance technology. All campus employees must adhere to this policy and to the established review/approval process established at each campus.

### IV – Access and Monitoring Process for UMS

Each campus will develop an appropriate review and approval process for individuals who are authorized to access, monitor, and view video recordings. This process will include:

a) The responsibility of the department to remove any Video Surveillance System access given to an individual at the time of separation from the university.

b) Video may only be monitored by authorized individuals. Other employees or third parties may not monitor or view video for any reason except as necessary in the course of an investigation or adjudication.

c) Selected campus and/or IT employees tasked with installation, maintenance, or adjustment of cameras, are approved for incidental access to the footage if such access is directly in conjunction with those aforementioned duties.

### V - Equipment and Network Maintenance

Troubleshooting, routine maintenance and minor repairs of equipment and software will be handled by each campus on an inspection schedule reasonably designed to ensure optimal equipment function. IT will work with the campus to help facilitate equipment repairs or replacements with an external vendor. Charges incurred by the vendor will be the responsibility of the campus or department owning the equipment. Additionally, maintenance and repair for
cameras that fall under “Exceptions” in Section I-Scope, will be the responsibilities of that technology owner.

V1 - Restrictions and Requirements
1. **Law:** All video surveillance installations are subject to federal and state laws. All recording or monitoring of activities of individuals or groups by university owned and authorized video surveillance installations will be conducted in a manner consistent with university policies and state and federal laws.

2. **Use of Recordings:** Information obtained from video surveillance installation shall be used exclusively for law and/or policy enforcement purposes, including student and/or employee discipline processes. Each campus must have established procedures in place to handle requests from non-university individuals or organizations for access to recorded media. These procedures must include a determination of whether or not the request is permitted under State of Maine Freedom of Information laws, federal law (i.e. FERPA) and/or university policy/practice. When appropriate, consultation with University General Counsel should occur.

3. **Non-Discriminatory:** All recording or monitoring will be conducted in a professional, ethical and legal manner. Such surveillance will not be based on race, color, religion, sex, sexual orientation, transgender status, gender expression, national origin, citizenship status, age, disability, genetic information or veteran status.

4. **Training:** All personnel with access to university owned or authorized video surveillance technology will be trained in the effective, legal and ethical use of such technology, as well as the expectation of confidentiality.

5. **Confidentiality:** University personnel are prohibited from using or disseminating information from university authorized video technology installations except for official purposes and/or court order. All such recorded and/or observed information is considered to be confidential and can only be used for official university and/or law enforcement business with appropriate campus approval.

6. **Location:** Every effort will be made in the location of video surveillance installation to protect personal privacy, and such installations are to be visible unless approval by the campus under exceptional circumstances. Except under exceptional circumstances, video surveillance will not occur in:
   - Restrooms
   - Locker rooms
   - Offices
   - Non-Laboratory classrooms

7. **Signage:** Areas where video surveillance is in use are to be clearly identified with signage that states “Video Surveillance in Use.” Signage is also to be at main entrances
to buildings where such surveillance is occurring. All signage is also to include contact information for interested persons with questions about the surveillance.

8. **Policy Breach:** Campus organizations, units and departments shall follow this policy and any procedures developed by that campus. Breaches of the policy may result in disciplinary action, in accordance with applicable handbooks and collective bargaining agreements.

9. **Retention:** Security camera recordings will be retained in accordance with the records retention policies of the State of Maine. This retention period may be extended or modified at the direction of the General Counsel or by law. Recorded media must be retained for at least 30 days unless there is an on-going investigation or presentation involving the media. Investigative agencies will determine the appropriate time period in those cases. All recorded media must be erased before disposal.

10. **Inventory:** Each campus is to maintain a history of each authorized video surveillance installation, unless there are exceptional circumstances, and this listing is to be available to the campus community upon request.

11. **Audit:** As directed by the leadership team of each campus, an external audit of the locations, use and effectiveness of all university video surveillance installations of public areas shall be conducted on a periodic basis.

The Governance Team shall maintain a record containing the following:

A) Camera locations;
B) Dates/times of monthly equipment inspections;
C) Dates/times of system or camera problems noted;
D) Dates/times of repairs to system or cameras including work performed and by whom; and
E) Dates/times stored video is accessed, including purpose for viewing, names of those who were present, and if video was duplicated.

12. **Inoperable Devices:** Installation of “dummy” cameras or other non-functioning video surveillance equipment is prohibited, as they may lead to a false sense of security.

13. **Policy Infringement:** Each campus will establish a procedure to address any concern about possible infringement of this policy.

14. **Audio Recording:** Audio recording of any kind is specifically prohibited by this Policy, unless authorized by court order or applicable law.

Approved by the Treasurer of the University of Maine System. Official copy on file in the Treasurer’s office.

August 6, 2019

Chief Financial Officer and Treasurer