RUTGERS
THE STATE UNIVERSITY OF NEW JERSEY

UNIVERSITY POLICY

Policy Name:	Security Technologies					
Section #:	30.1.11	**Section Title:**	Administration and Public Safety: Public Safety		**Formerly Book:**	N/A
Approval Authority:	Executive Vice President, Strategic Planning and Operations & COO		**Adopted:**	02/14/2019	**Reviewed:**	02/10/2020
Responsible Executive:	~~Executive Vice President, Strategic Planning and Operations & COO~~Executive Director of Public Safety / Chief of University Police		**Revised:**	02/10/2020		
Responsible Office:	University Public Safety		**Contact:**	policies@ipo.rutgers.edu		

1. **Policy Statement**

   Rutgers University is committed to enhancing and safeguarding the University's infrastructure and providing for the safety of the University community by integrating traditional and state-of-the-art technologies, while preserving reasonable expectations of privacy and operational efficiency. ~~The Security Technologies Unit~~Identity and Access Management reports to University Public Safety~~the Rutgers University Police Department~~, within the Division of Institutional Planning and Operations, and is responsible for all physical locks, keys, cameras, panic, and intrusion alarms.

2. **Reason for Policy**

   The purpose of this policy is to establish parameters for the authorized implementation and use of security technologies on University facilities to enhance safety and security as well as to establish minimum standards, where applicable. Further, this policy does not differentiate with respect to the source of funding used to purchase and/or install the equipment and technology.

3. **Who Should Read ~~t~~This Policy**

   All members of the University community.

4. **Resources**

   University Policy 30.1.8: Access to University Facilities
   University Policy 30.1.10: ID Issuance and Usage Policy
   ~~Security Technologies~~Identity and Access Management Website ~~– http://securitytechnologies.rutgers.edu~~
   General Inquiries - sectech@ipo.rutgers.edu or 848-445-4956

5. **Definitions**

Responsible Department – The University Department responsible for the locks and keys associated with its assigned infrastructure.

6. **The Policy**

I. Introduction

Rutgers University is committed to providing a safe environment through the use of state-of-the-art security features. ~~The Security Technologies Unit~~Identity and Access Management is responsible for authorizing and coordinating the use of security technologies for safety and security purposes at the University.

All security technologies shall comport with the University's standards.

II. Locks and Keys

In an educational institution there is a need to balance the accessibility and use of university facilities with the need to provide a safe and secure environment. Identity and Access Management~~The Security Technologies Unit~~ provides locksmith services to owned and controlled buildings and property statewide.

1. All locks and keys are the exclusive property of Rutgers, The State University of New Jersey and will be issued to faculty, staff, and students based on an established need for access. See University Policy 30.1.8: Access to University Facilities for more information. Excluded from this section are those locks maintained individually by departments for furtherance of department specific ends (e.g. padlocks utilized by Recreation Centers and department specific file cabinets.)
2. University Public Safety must be able to access all facilities for emergency response purposes. Accordingly, no University department may place a lock on a University owned, operated, or controlled facility (interior or exterior) without the express permission of the Director of Identity and Access Management ~~Security Technologies~~ or his/her designee. Departments found to be in violation may be responsible for repair and/or replacement costs made necessary to afford access.
3. All residential facilities will be locked twenty-four hours a day, except when residents are moving in or out of the facility. All other facilities will be locked whenever possible, dependent on use and scheduling.
4. The University reserves its right to change locks and keys as needed.
5. All keys must be returned to the responsible department or Identity and Access Management ~~Security Technologies Unit~~ upon termination of employment or enrollment.
6. Responsible departments will issue and track physical keys and maintain accurate access records. Access is issued in the strict trust that proper measures will be taken to ensure physical security of facilities.
7. Loss of keys and other access devices can result in great financial loss to the University and expose members of the University community to risk. Departments, units, and/or individuals may be held financially liable for losses incurred by the loss of University keys and other access devices including the cost of re-keying all locks compromised by the loss.

III. Cameras

Rutgers University employs video security technologies such as closed circuit television (CCTV) and cameras to deter crime, enhance personal safety, protect property, and to

assist the police in carrying out their public safety mission. These cameras remotely record activity on- and off- campus, may be subject to monitoring, and are used for investigative purposes during and after incidents that impact the community.

All University entities using video technologies (existing and new installations) for this purpose will adhere to this policy and the associated procedures.

1. Security camera usage (including purchasing of, installation, maintenance, monitoring, networking, etc.) must be conducted in a professional, ethical, and legal manner consistent with federal, state, and local laws and University policy.
2. All deployments of security technologies on campus (including, but not limited to, cameras, panic buttons, intrusion alarms, etc.) must be made in consultation with University Public Safety and Identity and Access Management ~~the Security Technologies Unit~~ prior to procuring equipment and installation. Requests for a security survey and recommendations may be made through the Identity and Access Management ~~Security Technologies~~ website.
3. Unless specified in a written agreement, Rutgers' departments are responsible for the purchase, maintenance, and upgrade of security camera equipment installed in their facilities.
4. Personnel involved in video security will be appropriately trained and supervised in the responsible use of this technology. Unauthorized use of video security may result in disciplinary action consistent with the rules and regulations governing employees of the University and may subject those involved to civil or criminal liability under applicable state and federal laws.
5. Information obtained through monitoring or recording will only be released when required by law or comparable authority.
6. Information and records (including recordings) are kept in the normal course of business. Such records shall be maintained for at least thirty (30) days after the last recording or until the footage is properly passed to a responsible official if an incident is reportable.
7. The existence of this policy does not imply or guarantee that video technologies will be monitored in real time 24 hours a day, seven days a week.

IV. Panic and Intrusion Alarms

Identity and Access Management ~~The Security Technologies Unit~~ installs and services electronic alarm systems. Remote monitoring is provided free of charge through the Rutgers University ~~Police Department's~~ 9-1-1 Communications Center.

It is recognized by this policy that certain facilities may be equipped with alarms subjected to central station monitoring. In those instances, the central station monitoring facility shall be directed to report activations to the Rutgers University ~~Police Department's~~9-1-1 Communications Center.

Facilities equipped with intrusion alarms shall certify annually a listing of contacts for their facility. Only certified contacts may contact Identity and Access Management ~~the Security Technology Unit~~ regarding maintenance.

V. Adherence

University Public Safety reserves the right to audit any department's use of security technologies, including installation, devices used, recording storage, and retention to ensure compliance with University Policy, state, and federal laws.