CRIME PREVENTION POLICY

Effective Date: May 10, 2006          Policy 1.23
Revised: January 1, 2011

Purpose and Scope

The University recognizes the value of established crime prevention practices in maintaining safe and secure campus environments. The University promotes incorporation of the International Association of Campus Law Enforcement Administrator's Recommended Crime Prevention and Campus Protection Practices for Colleges and Universities through the efforts of its individual campus safety crime prevention entities.

1. Facilities Design

Facility design or renovation, once initiated by University Construction & Planning, shall include crime prevention review, coordinated by the campus safety director, at the appropriate design stages in order to promote the concepts of Crime Prevention Through Environmental Design (CPTED).

2. Electronic & Physical Hardware

The University may utilize various types of electronic and physical hardware in protecting specific campus environments. These may include electronic access control, high security keying systems and monitoring systems. Monitoring may be used to help protect areas identified as requiring an increased level of protection such as parking lots, technology labs or cash handling & vending locations. Monitoring will not be used in any area where there is a reasonable expectation of privacy such as residence hall rooms, restrooms, private offices or locker rooms. Any use of cameras, video, or digital surveillance for investigatory purposes requires a request from the safety director and subsequent approval from the campus Executive Vice President.

3. Key Control

The University maintains key management practices that balance facility accessibility with security and safety. Exterior building key distribution is limited to the campus safety and facilities management departments. Interior key distribution and access programming is determined by the individual department head and the campus safety & locksmith departments. Duplication of university keys is strictly prohibited, and department heads are responsible for retrieving keys from employees who are terminating their employment or no longer require the use of issued keys. Each employee is responsible for maintaining security and custody of issued university keys. Lost or stolen keys and access cards must be reported immediately to the campus safety department.
4. Prohibition of Weapons

The possession or use of weapons or weapon replicas on university properties or at University-sponsored events is strictly prohibited. ROTC activities that may include weapon or weapon replicas require prior notification and approval from the campus safety department.

The campus Safety Department reserves the right to confiscate and secure weapons or weapon replicas found on campus.

5. Campus Student Special Events

The University recognizes the paramount importance of safety and security for campus special events. Special events are defined as those events and activities related to but not part of the formal instructional processes of the university.

Each campus shall coordinate special events in conjunction with the departments of student activities and safety. The individual campus shall address event security requirements, hours of operation, use or prohibition of alcohol, occupancy standards, risk management referrals, approval processes and other special considerations. All special events require prior review and approval by the departments of safety, student activities, and facilities.

Digital Imaging Monitoring

1. Purpose

This policy is developed for the purpose of implementing guidelines on the use of digital imaging monitoring equipment on ERAU property. This policy establishes principles and standards of behavior for ERAU employees about the use of monitoring systems in the workplace.

2. Guidelines

Digital imaging monitoring is not a real-time monitoring system and it is only to be used under the following circumstances.

A. To promote a safe environment through deterrents and crime prevention measures.
B. To provide the safety department with the means to conduct post incident investigations of crimes against persons or property that occur on university property.

3. Scope

This policy applies to all University assets where digital imaging monitoring cameras are installed. The authorization for the installation and location of digital imaging monitoring cameras lies with the Executive Vice President of each campus who works in conjunction with the director of campus safety.
4. Public Awareness of Cameras

For permanent installations of digital imaging monitoring equipment, signs will be posted in the area covered by monitoring informing the general public of the usage of monitoring cameras on campus.

5. Limiting Use, Disclosure and Retention of Personal Information

At no time will persons other than those designated by the campus safety department have access to the digital imaging monitoring recordings. Personal information contained on the recordings shall not be used or disclosed for purposes other than those for which it was collected.

Recordings from the digital imaging monitoring cameras will be kept for a maximum of 30 days unless required for the purposes outlined in this policy. Images retained for investigative purposes will be strictly managed with limited access. Digital imaging monitoring data remains the sole property of the university.

The focus of cameras used in monitoring on campus will not cover areas where there is an expectation of privacy.

6. Audits

The director of campus safety will report to the Executive Vice President for the campus at least semi-annually as to the effectiveness of the monitoring systems.

7. Retention/Disposal

The campus safety director or designee shall store all digital imaging monitoring data securely. Each storage device used shall be dated and labeled with a sequential number or other verifiable symbol.

Access to the storage devices shall be limited and controlled by the director of campus safety. Logs shall be kept of all instances of access to, and use of, recorded materials, and maintain an accurate audit trail.

Viewing of digital imaging monitoring data is strictly limited to the campus safety department and other appropriate personnel necessary to the investigation. Circumstances that warrant a review should be limited to instances where an incident has been reported/observed or for investigation of a potential crime.

8. Temporary Installations

The University recognizes that certain crime or safety and security conditions may warrant the temporary installation of digital imaging monitoring equipment to identify, without public notice, unknown suspects committing infractions on university property. Requests for temporary
installations first require a safety department investigatory incident report documenting the condition. The campus safety director will then review the case with the Executive Vice President for the campus and obtain approval before proceeding with temporary installations.

9. Disclaimer

Digital imaging monitoring does not guarantee that someone on university property is safe from crime. There should be no expectation that the digital imaging monitoring system is being monitored 24 hours, seven days a week and that the safety department is going to observe and respond to a crime in progress.

10. Covert Use

Covert Use of digital imaging monitoring systems:

1. The authority for the approval of covert use lies with the Executive Vice President for the campus. Covert use of surveillance systems shall be highly restrictive and temporary in nature.
2. All requests for covert use shall come from the director of campus safety to the Executive Vice President for the campus.
3. The request shall be in writing and document the justification, location, time period for the covert use. This request shall include if the covert use is going to be real-time monitoring.
4. If approved, the Executive Vice President for the campus will sign the request and note any additional restrictions he/she deems appropriate.
5. The director of campus safety will assure that all procedures are followed as outlined in the non-covert use section of this document. Public notice is not required for covert use operations.
6. The director of campus safety will assure that all equipment is removed at the end of the approved time period. The director will also make sure that all recordings are destroyed, unless the recording is to be used as evidence.

Responsible Authority: Associate Vice President for Safety