



# **UW-Madison Police Department**

## **Policy: 91.1**

**SUBJECT: PHYSICAL SECURITY RISK ASSESSMENTS**

**EFFECTIVE DATE: 12/31/11**

**REVISED DATE: 09/01/12; 01/18/18; 05/16/18; 02/19/20**

**REVIEWED DATE: 04/01/14; 01/24/19**

**STANDARD: CALEA 91.1.1, 91.1.3, 91.1.7, 91.1.8**

---

### **INDEX:**

- 91.1.1 PHYSICAL SECURITY RISK ASSESSMENT
- 91.1.2 SECURITY CAMERAS
- 91.1.3 UNIVERSITY BACKGROUND INVESTIGATIONS

### **POLICY:**

The UW-Madison Police Department Infrastructure Security Unit provides physical security risk assessments to our campus partners upon request, or when risks are identified by UW-Madison Police Department staff. Physical Security Risk Assessments range in size, scope, and complexity, and require input and assistance by community stakeholders.

### **DEFINITIONS:**

“Risk assessment” refers to the quantification of liabilities to a particular location, event, or individual.

### **PROCEDURE:**

#### **91.1.1 PHYSICAL SECURITY RISK ASSESSMENT**

- A. The basic foundation of the infrastructure security function includes physical security risk assessments and analysis of the information. Analysis of past data indicates what has happened and provides insight to the potential for future criminal activity. The following shall provide guidelines for conducting physical security risk assessments:
- B. Factors to consider include, but are not limited to: frequency of past occurrences, the criticality of the event and loss or replacement costs, crime and incidents reports, case dispositions, alarm reports, previous risk assessments, vehicle and personal accident reports, potential weather and geographic events, physical and building issues, the surrounding demographic environment, possible negligent human actions or criminal and terrorism actions.
- C. A documented physical security risk assessment is required every four (4) years at the following locations:
  - 1. Select Agent Labs
  - 2. Mechanical Engineering Reactor Lab
  - 3. Kohl Center
  - 4. Camp Randall
- D. Risk assessments shall evaluate risks to campus community from criminal activity, risks to campus community from accidents, risk of property loss to the institution and individuals, and liability issues. Each assessment shall contain an analysis conclusion with recommendations for mitigation. Recommendations shall be forwarded to the appropriate individuals responsible for the facility.
- E. Staff conducting security surveys or risk assessments shall be appropriately trained as defined by the department.

#### **91.1.2 SECURITY CAMERAS**

- A. Security cameras are effective in reducing crime and aiding in the identification of criminals and situations where the public may need assistance. The following shall provide guidelines for the installation and review of security cameras:
- B. The Director of Security Video Operations or designee shall provide input to new building and remodel project managers on security camera locations. This is based upon department need, criminal activity, nature of building occupancy (controversial research, sensitive or high risk items, etc.) Camera locations include, but are not limited to: exterior entrances, loading docks, elevator lobbies, locations with cashiering functions, and other locations as determined by the building occupants and guidance by Director of Security Video Operations. Pan-Tilt-Zoom cameras (PTZ) may be specified for large lobby/atrium/public interior or exterior spaces. Where the Department determines a PTZ camera is the best option, the camera will be a high resolution I.P. PTZ camera.

- C. Security cameras record on motion, but are not actively monitored unless specific arrangements have been made with the Department Communications Center or the Director of Security Video Operations. The requesting Department on campus should have an identified need to monitor the camera and a time period for monitoring. In the event of an alarm at an active camera location where the alarm and the camera work together, the law enforcement dispatcher shall review the video feed and notify responding officers of any unusual occurrences and or suspect information. When there is a critical incident on campus the Emergency Camera Response Plan is implemented so that the cameras are used efficiently to maximize the safety of everyone involved in the incident.
- D. If at any point a security camera fails or is tampered with, an administrator is automatically notified. This notification is disseminated and stored electronically in accordance with UW-Madison records retention schedule. If the camera issue cannot be resolved in a simple manner, the Director of Security Video Operations or designee shall be coordinate and maintain documentation of the maintenance and/or repair for all centralized security video cameras.
- E. The media retention schedule for security camera footage not deemed evidentiary is 120 days. Requests made by other law enforcement agencies to review video security camera video footage shall be coordinated and tracked internally through the Director of Security Video Operations or designee.
- F. Departments on campus that have a Web Client account, maintain an active directory account and have received training may review the video from the camera locations at their facility.
- G. The level of access and/or restrictions to the camera system for UWPD employees is determined by the nature of employment. Initial and refresher training on the operation of the system is coordinated through the Director of Security Video Operations or designee. Due to the sensitive nature of accessing security camera footage, users are not granted appropriate access until completion of initial training(s). This training covers access privileges and the responsibilities of employees.
- H. Video footage is considered a record of the department and request to view or obtain copies of the footage shall be released to outside requesters in accordance with department directive 82.2 Field Reporting and Management.
- I. The Director of Security Video Operations or designee shall conduct an annual evaluation of incidents and camera locations to ensure timely adjustments are made.

### **91.1.3 UNIVERSITY BACKGROUND INVESTIGATIONS**

- A. The Department fingerprints employees of select agent, irradiator, and reactor labs. The prints are sent to the Federal Bureau of Investigation.
- B. The Department conducts criminal history and law enforcement contact checks on staff working on high level, controversial research. These background investigations are conducted in an effort to determine trustworthiness and reliability of the persons in those assignments.