

<b>University Enterprises, Inc. Policies and Procedures</b>	<b>Policy No. 2060</b>
<p><b>Section:</b> Business Services Department</p> <p><b>Policy:</b> Video Surveillance Policy</p> <p><b>Effective (or) Revised</b> December 7, 2018</p>	

## Policy Name

### I. PURPOSE

To provide management with policies and regulations governing UEI video surveillance.

### II. SCOPE

This policy applies to all UEI personnel, including central administration and sponsored programs.

### III. POLICY

#### I. Background and Purpose

In an effort to promote security, safety and compliance with policies supporting the same, University Enterprises, Inc. ("UEI") may elect to use temporarily and/or permanently-installed video surveillance technology and equipment in accordance with the provisions of this policy. Such technology and equipment may be used to record and capture video images but shall not be used to record or capture audio content. The contents of any captured video images shall not be exploited for purposes of profit or commercial publication without appropriate justification and the express written consent of any individual whose likeness appears in the captured video images.

In order to promote uniformity in the administration of video surveillance measures and to mitigate the opportunity for interference with individual privacy rights, this policy is established to define the physical areas subject to video surveillance, and rules relating to the establishment of video surveillance, viewing of recorded media, and retention of the recorded media

#### II. Policy and Regulations

##### A. Areas Subject to Video Surveillance

1. Video surveillance may be used to monitor any portion of UEI's operations including but not limited to interior and exterior doors providing access to facilities owned or operated by UEI, common areas open to the public or UEI employees, food preparation centers, storage facilities, cash handling areas, and any other area that is open or accessible space within the sight and hearing of coworkers, visitors, supervisors, customers or the general public.
2. Notwithstanding the foregoing, video surveillance shall not be used to monitor physical areas in which a member of the public or an employee would have a reasonable expectation of privacy such as changing rooms or restrooms, offices that have a closing

---

door, and other enclosed, discreet areas to which the public's and employees' access is limited or restricted.

#### **B. Approval Process**

1. New requests for use of video surveillance technology and equipment in any building or facility owned or operated by UEI shall be subject to the approval of UEI's Executive Director.
2. The request shall include a justification for the need for such surveillance, the extent or duration of the surveillance, a description of the physical areas subject to video surveillance, the proposed location for secure storage of media, and a media retention schedule.
3. The Executive Director may approve or disapprove a request in whole or in part.
4. The Executive Director will periodically update the UEI Board of Directors or Executive Committee on UEI's use of video surveillance technology and equipment.

#### **C. Notification of Video Surveillance**

1. Prior to activating any video surveillance system, UEI will place signs easily visible in areas subject to the video surveillance in order to notify employees and members of the public that the area is or may be under video surveillance.
2. In no case is covert video surveillance permissible.

#### **D. Viewing of Recorded Media**

1. Only individuals having a legitimate need to view the live images or recorded video media may be permitted to do so.
2. The director of the operating unit that is subject to video surveillance and the Executive Director may view video surveillance media.
3. Other individuals having a "legitimate need" may be permitted to view the media upon the advance approval of the Executive Director, with the exception that the media may be directly provided to a law enforcement official upon request, or to a third party in compliance with a subpoena or court order.
4. Legitimate need includes but is not limited to reviewing recorded media by those who are either responsible for 1) investigating actual or suspected: injuries to persons, criminal activity, or damages to or losses of property, or 2) taking action to make corrections in the workplace designed to avoid such incidents.
5. The Executive Director will determine if legitimate need has been demonstrated.
6. The media and images or data contained on the media shall be treated as confidential to the extent allowed by law.

#### **E. Retention Period for Recorded Media**

1. If video media may contain evidence of a crime or attempted crime, the media will be maintained as may be directed by law enforcement officials.
2. Otherwise, video surveillance media shall be kept for a reasonable period that would allow enough time for a crime, accident or injury to be reported.

3. Recorded media that does not contain evidence of a crime, accident or injury may be maintained for a maximum of sixty (60) days, or longer as may be approved by the Executive Director.
4. The recorded media shall be stored in a secure location. Video media will be destroyed or recycled upon the end of the retention period.

**VI. RELATED POLICIES**

N/A - None