


Administrative Policy

Title: **Monitoring Research and Clinical Equipment**

Source: University Police Department, Electronic Security Division

Prepared by: Director, Electronic Security Division, University Police Department

Approved by: Donald M. Elliman, Jr. 
Chancellor

Effective Date: April 18, 2016

Replaces: April 1, 2009

Applies: University of Colorado Anschutz Medical Campus

A. Introduction

1. This policy is applicable to all University of Colorado research and clinical equipment that, because of contents need monitoring for equipment status and temperature, and condition as detailed in this policy.
2. For buildings/sites that are on the University of Colorado Anschutz Medical Campus (Anschutz) including Children's Hospital Colorado, University of Colorado Hospital, Fitzsimons Redevelopment Authority, University Physicians Inc., the Electronic Security System will monitor equipment, where the university data network is or can be available. The Electronic Security Division will install and maintain the alarm-monitoring infrastructure in the research, storage, and clinical facilities to support equipment monitoring except in expressly waived areas reviewed by Facilities, University Risk Management, and Electronic Security Division and showing a benefit beyond available systems.
3. For all other buildings/sites, equipment owners will install independent equipment monitoring systems consistent with the standards for locations identified in A.2.
4. Where research or clinical processes maintain products in monitored containers and require a particular level of physical security such as "Scheduled" drugs, certain pharmaceuticals, high-risk chemicals, etc., the monitored container will also provide the requisite security components, alarm, and notification protocols.

B. Table of Contents

- A. Introduction
- B. Table of Contents
- C. Purpose
- D. Policy Statement
- E. Standards
- F. Equipment Owner Responsibilities
- G. Electronic Security Department Responsibilities

C. Purpose

1. The policy defines "monitored equipment" as research or clinical equipment vulnerable to temperature change losses or mechanical failure and their respective contents connected to the Electronic Security System or an independent monitoring system.
2. This policy will identify the responsibilities of the equipment owner and the Electronic Security Division relative to the monitoring of certain equipment.
3. This is a requisite supplement to other actions taken by Equipment Owners to protect research equipment and contents.

This policy requires owners of the equipment within the policy's scope to connect to the university Security system if on campus as described in A2 or an appropriate independent monitoring system if off campus as described in A3, to receive warning of temperature changes or other equipment alarms to prevent damage to or loss of equipment contents. Failure to connect to the system may limit reimbursement of losses

D. Policy Statement

In order to preserve and protect the integrity of University research and clinical support, this equipment monitoring policy is hereby established.

This policy requires the monitoring of certain research or clinical equipment vulnerable to temperature change losses or mechanical failure. Failure to connect to a monitoring system may result in partial reimbursement or denial of any claims submitted for losses of research material, clinical support medications, or other covered materials contained within the equipment.

Equipment encompassed by this policy includes but not limited to:

1. All ultra-low temperature (ULT) -80°C freezers, as well as -20°C, -4°C freezers; other refrigeration equipment, incubators, liquefied gas containers protecting ULT units, with contents of \$10,000 or more in value and
2. All equipment that contains items that when warmed to ambient temperatures will present a health threat or other safety issue and
3. All equipment that contains items whose replacement is difficult or not possible.
4. Owners of equipment not directly included within the scope of the policy may enroll equipment in the program to provide the early warning of risk to equipment contents.

University Risk Management (URM) recommends that to minimize equipment contents losses due to temperature variation or a mechanical failure of the equipment, the owners should spread contents among various equipment units, whenever possible. This will minimize the replacement cost of the contents of any one unit. In no case should an individual unit's contents replacement cost exceed \$2,000,000. Contact University Risk Management for specific insurance information at urmucddirs@cu.edu.

The Vice Chancellor for Research, the Senior Vice Chancellor for Administration and Finance, or the Chancellor must approve exceptions to this policy where URM insures equipment and its contents against loss.

E. Standards

1. All new ULTs purchased for use in Anschutz facilities will have internal alarm sensors tied to a communications block in the unit to facilitate the connection of those alarms to the remote monitoring. The Procurement Service Center (PSC) has the ULT specification requirements and help ensure internal alarms are included in the purchase. There is no procurement standard with PSC for the purchase of other freezer or refrigeration equipment, as those products do not normally come with internal alarm options.
2. Equipment Owners of existing research and clinical equipment, within the scope of this policy, should upgrade or repair affected equipment to accommodate monitoring. Facilities Management or commercial vendors can evaluate -80°C units for sensor installation and connections as some older ULTs and those brought with researchers from outside labs may not have internal sensors or a central connection point. Other freezers typically do not ship with alarm sensors installed. Where equipment lacks internal alarm sensors, it may be possible to add an external power and temperature sensor with a probe. The Equipment Owner must first coordinate the placement of equipment to ensure the appropriate circuits, sockets; electrical support, etc. are available for the desired location. Facilities Management will work with each equipment owner on the installation or relocation of electrified equipment within university owned and managed buildings.
3. On the Anschutz campus, the Electronic Security Division has installed a wiring backbone for this purpose in most areas within the research facilities and clinical areas on campus. Nonetheless, Security will connect all specified research or clinical

equipment located outside these spaces to the security alarm system. Requisite for connection and enrollment into the campus system is presence of campus network and sitting proximate to the Anschutz campus. Security may assess a nominal charge to cover wiring and parts where the unit is a significant distance from the security system.

F. Equipment Owner Responsibilities

1. The "Equipment Owner" is the individual responsible for the custody, maintenance, and care of the equipment, its contents, and any related research products or processes. This is typically the Principle Investigator or Clinician overseeing research and patient care respectively.
2. The Equipment Owner must first coordinate the placement of equipment to ensure the appropriate circuits, sockets; electrical support, etc. are available for the desired location. Facilities Management will work with each equipment owner on the installation or relocation of electrified equipment in university owned or managed buildings.
3. The owner of any equipment not proximate to the Electronic Security System may move it to a covered area or help fund the extension of the electronic coverage to the equipment location. The exception to this will be the lack of appropriate electrical power or circuits or available equipment space in a linear equipment room (LER), or the lack of Electronic Security System connections. In these cases:
 - a. Facilities Management will review the possibility to add either power outlets or circuits, if power is available from the closest power panel.
 - b. Electronic Security will extend the network to the equipment's location or to where Facilities Management has installed new power receptacles.
 - c. If the equipment is located in the laboratory due to a lack of space in the LER the department administrator may relocate other items using LER wall space to allow the equipment to access the correct power receptacle and security network.
 - d. Newly constructed laboratory and research facilities will have the infrastructure for monitoring research equipment in place upon completion of construction.
4. Any cost associated with the purchase, repair, or upgrading of equipment is the financial responsibility of the Equipment Owner.
5. Equipment Owners should consider mounting a daily temperature log or performance checklist to document equipment stability.
6. As a best practice, University Risk Management and Environmental Health & Safety (EHS) strongly recommend that the Equipment Owner maintain a reasonable inventory of contents and the approximate replacement value of each item in order to: evaluate the risk the equipment and its contents present; facilitate any claims for losses; provide critical information regarding safety relating to contents and quantify the environmental risks related to the equipment and their contents. EHS offers both a biological inventory

(www.ucdenver.edu/BioInventory) and chemical inventory (www.ucdenver.edu/ChemInventory) web modules for Equipment Owners and researchers to maintain their freezer inventories. Contact EHS for assistance at Chemical.Inventory@ucdenver.edu or Biological.Inventory@ucdenver.edu.

7. The Equipment Owner is responsible for providing current contact information for all persons associated with the monitored equipment and to ensure the contact information is updated immediately when the information changes. The Owner should review the information quarterly. Security will provide necessary forms, which seeks this data:
 - The staff members' full name
 - Staff members' campus phone number
 - Cellular telephone's email address, a text capable alphanumeric pagers email address, and/or
 - An email address checked during non-work hours.
 - Equipment Owners can forward changes to Equipment.Monitoring@UCDenver.Edu
8. For equipment monitored by the Electronic Security System, the Equipment Owner will attach a copy of the security form located at <http://www.ucdenver.edu/about/departments/UniversityPolice/ElectronicSecurity/SecurityBadgingOffice/Pages/EquipmentMonitoring.aspx> on each piece of monitored equipment with current contact information that is on file in the Electronic Security. This allows anyone seeing an alarm condition to initiate owner notification immediately. Security recommends this step also for off campus locations.
9. The Equipment Owner should be familiar with the fragility of container contents so the temperature alarm calibration and set points, adjusts, and programs the freezer alarm panel considering response time, availability of other containers, degradation of contents, etc.
10. The Equipment Owner should respond in person or send a representative capable of investigating and/or correcting the cause of the alarm after receiving a notification of an alarm. Response may include the relocation of equipment contents to other support equipment to maintain the appropriate condition or temperature. Facilities Management maintains a limited number of short-term loaner ULT freezers for this purpose. Call Facilities Dispatch at (303) 724-1777 or at Dispatch@UCDenver.edu for assistance. It is very important to call the campus information hot line at 1-877-INFO-070 (or 1-877-463-6070) first to determine if there is a building or system-wide outage. Responders should check their respective email accounts for information about wide outages, specific freezer or multiple equipment alarms. The Information hot line will be updated with pertinent information if there is a building or systemic outage. However, an outage does not preclude the need for the equipment owner to respond and otherwise preserve freezer contents.
11. Response to alarms and the protection of research and clinical processes, equipment, and materials are the sole responsibility of the Equipment Owner, though the owner may delegate or share response to or with qualified staff members.

12. The Equipment Owner is responsible for minimizing alarms by providing reasonable preventive maintenance to the equipment to ensure its stability, reliability, and lack of false or nuisance alarms. The Equipment Owner should maintain a service agreement with a qualified service provider and ensure service providers have access to the equipment for servicing. Facilities Management can provide such services for a fee.
13. If Security cannot activate and test the equipment alarm, due to the condition of the equipment, such as having clogged filters or inadequately charged batteries, it is the responsibility of the equipment owner to have the necessary maintenance performed to take the equipment out of alarm so that Security can alarm the equipment. The Owner should contact security Equipment.Monitoring@UCDenver.Edu when the equipment out of service for any reason so that the alarms may be turned off for that period.
14. For locations as defined in A.3, Equipment Owners will be responsible for securing the services of a third party provider to monitor equipment to ensure the requirements of this policy are met.

G. Electronic Security Responsibilities, as defined in A.2 above:

1. The Electronic Security Division of the University Police Department is the university entity responsible for defining Electronic Security standards applicable to Anschutz, maintaining the Electronic Security System, and coordinating system monitoring with the equipment alarm responders.
2. Electronic Security will provide continuous monitoring of installed alarm status on monitored research equipment to ensure operability of the system but not for response to the alarms generated. Should an alarm remain active for an extended period, Security will attempt to contact the owner to validate the equipment condition and status.
3. The Electronic Security System will be programmed to cause emails to be sent to specified staff members' specified email accounts, cellular telephones, and/or text pagers advising them that an alarm is triggered for specific monitored research equipment.
4. Electronic Security personnel are not qualified to respond to equipment alarms but can work with owners to test the alarm system. Response to alarms is the responsibility of the Equipment Owner.