SEMD-SD-RO-210 – Security Systems

1. Purpose

The purpose of this procedure is to develop standard and consistent guidelines relating to the installation, testing, operation and maintenance of security systems at Fermilab. The use of these systems is to enhance the safety of employees, users, and visitors and to protect laboratory property.

2. Scope

This procedure applies to all Security Department personnel who, within their assigned duties, are required to conduct security system testing, system installations, perform basic maintenance, operation and the monitoring of security systems.

3. Applicability

This policy applies to all uniformed members of the Fermilab Security Department, full-time and part-time employed by Fermi Research Alliance (FRA) for Security Services.

4. Effective Date and Date Reviewed/Updated

This policy went into effect on June 9, 2016 and its update was effective on July 18, 2024.

5. Policy

The use of Video Assessment Surveillance Systems (VASS), Physical Access Controls Systems (PACS), and Duress alerts are to reduce any perceived or actual risk of harm to personnel and property. Security systems shall contain a list of camera locations, card reader and controller locations as well as system panels. All security system information is kept on file on the secure server. VASS and PACS can be monitored via software on selected computers from authorized user accounts.

6. DURESS SYSTEMS

6.1. Duress Alerts (Personal Safety)

6.1.1 There are several Duress Alerts located within Wilson Hall, Site 39, and Aspen East. These include Campus Access Office (WH1NW), Atrium Security Help Desk, Cashiers Office (WH4NE), Medical Office (WHGF), EOC (WHGF), Abri Credit Union (WHGF), HR Offices (WH15), and Site 39 ES&H. Aspen East has 6 units located in the Badging Offices and 1 in the Housing Office. Users are also instructed to call the emergency line if possible. Duress alerts annunciate in the Security Operations Center via the FIRUS system. Site security personnel are dispatched and cameras, if located in the area, are monitored and any relevant information is relayed to responding units.

6.1.2 Duress alerts are discouraged and no longer being provided.

6.2. Security Alarm System

Security systems are not in use on site, with the exception of the Abri Credit Union in Wilson Hall, which is in leased space and required by the lessee. Outside local law enforcement agencies are contacted in the event of an alarm. The SOC monitors the VASS and provides communication updates with responding agencies.

6.3 Video Assessment and Surveillance Systems (VASS)

VASS may be used for monitoring and/or recording public areas, parking lots, access gates and site buildings for deterring theft or other criminal activities and enhancing personnel safety. Security cameras augment the security officers and aid in security patrols of the site. VASS systems meet the requirements of the Prime Contract CLAUSE I.10G – FAR 52.204-25 PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT.

6.3.1 Security Camera(s) are registered on the Fermilab domain and are compliant with Fermilab's Computer Security policy.

6.3.2 The security technician will assess, install (according to manufacturer specifications), maintain and troubleshoot VASS components as necessary.

Hardware/firmware/software updates are updated routinely. The security technician will repair/replace any cameras which fail within 72 hours if possible, or security officers will be required to patrol the area more frequently.

6.3.3 Security cameras are viewed in the Security Operations Center by Emergency Operator/Dispatchers in support of operations in accordance with established procedures. Camera views may be changed by the Emergency Operator/Dispatchers to aid security officers in the event of a security incident or alert security officers to any suspicious activity. Due to the high volume of security cameras in use, it is not intended or expected that all security cameras be constantly monitored in real time. If a camera fails, the camera display will show "camera disconnected" message in the display window. The Emergency Operator/Dispatcher will make appropriate notifications.

6.3.4 Requests for access to view or obtain recordings shall be made to the Physical Security Manager or his/her designee and/or the Legal Office. Only the Physical Security Manager or his/her designee may authorize release of recordings to non-security department personnel. Requests for video recordings shall be documented in the case report.

6.3.5 Recorded images shall be retained for a period of 45 - 90 days then recorded over unless there is a demonstrated business need or requirement for an ongoing case report or investigation. Recordings are stored on 5 dedicated servers located inside a PACS enabled server room at FCC. Remote access to the server is limited to the Deputy Physical Security Manager, the Security Technician, and the server support team who installs updates/patches as needed. Administrative access to the camera management software is limited to the Security Technician, Deputy Physical Security Manager and the Physical Security Manager by password protected user accounts. Other authorized users can view certain cameras based on user permissions and their demonstrated need.

6.4 Physical Access Control Systems (PACS)

PACS solve the limitations of mechanical locks and keys. A wide range of credentials can be used to replace mechanical keys. Fermilab uses the ID badge as a credential for card access and the card readers are in the process of being updated to accept HSPD-12 credentials as well. The PACS grants access when the ID badge is presented, and the card is in the clearance group for the area in which the card is presented. When access is granted, the door is unlocked for a predetermined time and the transaction is recorded. When access is refused, the door remains locked, and the attempted access is recorded. The system will also monitor the door and record on the message log if the door is forced open (bypassed reader by using a key) or held open too long after being unlocked. Fermilab has contracted with Johnson Controls, Inc. to provide PACS in many of its buildings. Johnson Controls, Inc. uses proprietary hardware and software.

6.4.1 Automated Access Control System Installations

6.4.1.1 Requests for PACS are made to the Security Department who arranges with the vendor, Johnson Controls, Inc., to provide a quote for PACS.

6.4.1.2 A Security Department staff member or Security Technician will meet with the vendor and building manager at the location for a walk through to obtain the exact location and necessary information the vendor will need. The vendor will also include their subcontractor electrician and locksmith on the walk through of the area.

6.4.1.3 The vendor will provide a quote to requestor and the Security Department. The requestor will process a requisition for procurement if they are going to proceed with the installation.

6.4.1.4 Once the PACS is installed according to manufacturer specifications, it must be programmed into the PACS database. C.Cure9000 is the software in use at Fermilab. The vendor will program the card readers in the database, identifying door numbers and using the established

nomenclature of the existing clearance group names. The Deputy Physical Security Manager, Security Technician and the Physical Security Manager are system administrators. The Security Operations Center staff are users who have limited privileges within C.Cure9000. All users in the Security Operations Center have the monitoring station visible at their workstations to view real time events.

6.4.1.5 The Security Department will follow SEMD-SOC-RO-213 for granting building clearances.

7. Definitions

7.1. Duress Alert – a threat alert or distress signal usually activated manually through a portable or fixed device which sends a signal through FIRUS to the Security Operations Center indicating an immediate threat to the safety and security of personnel within the area of the alert.

7.2 FIRUS – Fire Information Reporting and Utility System.

7.3 PACS – Physical Access Control Systems

7.4 Shall – the use of the word "shall" indicate a required action.

7.5 VASS – Video Assessment and Surveillance System

8. Responsibilities

8.1. The Physical Security Manager is responsible for ensuring all Security Department personnel understand and follow this procedure.

8.2 The Security Operations Center Emergency Operator/Dispatchers are responsible for monitoring security systems. All security system malfunctions shall be documented on an irregularity report and notification shall be made to the duty Security Supervisor.

8.3 The Security Operations Center Supervisor is responsible to test the portable duress alerts and maintain test records.

8.4 The Security Supervisors – are responsible to ensure the security officers and/or Security Operations Center Emergency Operator/Dispatchers are making checks of the area(s) via physical patrol, PACS, and/or VASS.

8.5 The Security Technician – is responsible to register, install, maintain, troubleshoot and update systems.

9. Authorities

9.1 Performance Assurance Program (PAP) Plan
9.2 DOE O 470.4B Safeguards and Security Program
9.3 SEMD-SOC-RO-213 Keys, Card Access and Lock Service

10. Owner

The Physical Security Manager is the owner of this policy.

11. Review Cycle

This policy shall be reviewed annually or more frequently, as needed.

12. Communication Plan

The requirements of this policy shall be communicated by the Physical Security Manager to all Security Department personnel, and periodic training shall be provided. This policy shall be available in the Fermilab Security Department policy database.