SEMD-SOC-RO-213 – Keys, Card Access, Lock Services, and Terminating Personnel

1. Parent Policy and Related Policies/Procedures

SOC-RO-213, Key and Lock Services

2. Purpose

The purpose of the Key, Card Access and Lock program is to ensure that employees, users and affiliates, and subcontractors hold access and keys appropriate to their actual needs and to maintain accountability of all outstanding keys. This procedure also provides guidance and instructions in the retrieval of government property to include keys and Fermilab badge from terminating personnel.

3. Applicability

This procedure applies to Security Operations Center personnel and Locksmith.

4. Effective Date and Date Reviewed/Updated

This procedure went into effect on 09/01/2016 and its update was effective on 07/18/2024.

5. Procedure

a. Issuance of building office keys.

Requester is to fill out a Key/Lock Request through the Apex Security Key & Lock Request System. The request will go through an online workflow process notifying the supervisor and requesting approval from the Building Manager or the Division controlling the area for which he/she is requesting access. The current list of persons authorized to approve key issuance for each Division is maintained in the Apex Security Key & Lock Request System.

b. Type of key issuance

Personal keys are keys issued to an individual for personal use. Normally only one copy of each key will be issued. All keys will be stamped with a unique identifier consisting of the keys system identifier number and either the responsible person's badge number or a Duty Ring designator.

Duty ring keys are keys issued for use on a group duty ring. The keys will be stamped with a duty ring identifier to include the suffix "DR". If the same group has multiple identical duty rings the identifier will have a suffix that indicates the quantity of rings (i.e., "--DR1", "--DR2", etc.). The keys will not bear the requester's badge number, but they will be listed in the database as being the responsibility of the requester. The requester must describe the need for and use of the duty ring. The Security Access Specialist will ensure the Lock/Key Request for the duty ring key(s) is routed to all appropriate Divisions.

Multiple copies of same key number must be approved by the Reviewing Officer. The keys will be serialized using "/1", "/2", etc., after the key number ("/1" will indicate the second copy of the same key badge number). The keys will be stamped with the requester's badge number.

c. Processing a Key/Lock Request

Upon receipt of a Key/Lock Request notification email, the Security Operations Center Supervisor will verify that the proper key is requested for that area. The key request will automatically be assigned a request number in the Apex Security Key & Lock Request System. All building keys are issued, and locks installed under a controlled process. Designated Division and Project personnel approve each issuance or installation. Key types include Master, Submaster, Sub-submaster, and individual keys. Every effort is made to ensure the lowest level key is issued for the requested area(s).

If the request is for duty ring keys, the Security Operations Center Supervisor will note that in the SOC Comments section of the Key/Lock Request.

If the request is for rekeying a group area or facility, one Key/Lock Request may be used. The requester will be required to supply all needed information and drawings to the Reviewing Officer. The Security Operations Center Supervisor will send it to the Reviewing Officer.

The Reviewing Officer will survey the request to determine that the key requested will grant access to the specified area without also providing access to areas for which the requester is not approved.

The Reviewing Officer will also assess the requester's current key holdings and, when possible, reduce the quantity of keys held by an individual by assigning a different level of key, provided no unwarranted increase in access is granted. He/she will make a note for the Locksmith's information about any special stampings for duty ring or multiple issuance keys.

The Reviewing Officer may direct that additional information be obtained. He/she will approve or disapprove the request and return it to the Security Operations Center Supervisor. If disapproved, the Reviewing Officer will note the reason on the request and contact the requester, or his/her supervisor in person. When full review and approval are complete, the request will be released to the Locksmith.

The Locksmith will fabricate keys requested, stamping them with key identification information and the badge number of the requester. The Locksmith will complete their workflow process and will transport the keys to the Security Operations Center.

Keys may not be signed for by any individual other than those to whom they are assigned. The Reviewing Officer may make exceptions to this policy.

The Security Access Specialist will complete the workflow process which will automatically email the requester that their keys are ready for pickup. When the requester comes to pick up keys, verification will be made that the correct information has been stamped on the keys. The requester must electronically sign and acknowledging receipt and responsibility. The Security Operations Center employee issuing the keys will complete the process by logging the information in the Apex Security Key & Lock Request.

If the keys have not been picked up within two (2) weeks, the Security Access Specialist will email or mail a second written notice to the requester. At the discretion of the Security Operations Center Supervisor, a copy of the second notice will be emailed to the requester's Division (if employee) or the experiment spokesperson (if visitor). Every attempt will be made to have the requestor pick up the key(s) prior to their destruction at the end of six months.

d. Installing Locks

Requester is to fill out a Key/Lock Request through the Apex Security Key & Lock Request System. He/she must then provide the number of locks requested and clearly describe the locations in which they are to be installed, including room and/or door numbers where available. The reason for needing new locks must be stated. Authorizations, reviews, and approvals are the same as above.

It is recommended that when locks are to be installed that will affect employees' access to a building or area, prior arrangements are specifically made with the Reviewing Officer. He/she will work with the requester to establish a timetable for work that will provide ample time for obtaining keys for employees and informing them of the change.

e. Processing special lock or key requests

The standard procedure for cutting system keys and installing system lock cores can take several days, involving numerous notifications as described in this procedure. However, there are situations that require faster action than is possible by the standard procedure. These include, but are not limited to, safety concerns, beneficial occupancy to new construction projects, security drills/inspections, and specific operational needs.

Issue/installation of temporary keys/cores, where time and/or circumstances do not permit the standard lock/key request procedure to be followed, and the issuance/installation are based on a temporary need.

A key request will be filled out noting requester, reason for issuance/installation, and the time frame the key or core is needed.

The Reviewing Officer or his/her designee will be notified and will either approve, amend, or deny the request. They may also require additional notifications be made.

The Locksmith will be given written instructions that are noted in the SOC Comments section of the Apex Security Key & Lock Request System on how to mark the key/core and to whom to deliver it or where to install the core.

The key(s)/core(s) will be returned to/removed by the Locksmith for destruction on the date noted on the key/lock request. The Locksmith will note the destruction/removal in the comments section and will destroy the key.

The key/lock request will then be sent to the Security Operations Center for inclusion in the database as a key/lock issued/installed and/or returned/removed.

Issue/installation of permanent keys/cores, where they are needed sooner than the standard procedures allow:

1. A key/lock request will be filled out noting the requester. The Security Operations Center Supervisor or his/her designee will review the request.
2. The Security Operations Center Supervisor or his/her designee will consult with the responsible signatories for the appropriate Division.
3. If the request is denied, the requester will be notified to submit the request through the standard key/lock procedure.
4. If the request is approved, it will be forwarded to the Locksmith. The Locksmith will cut the key or combinate/install the core following standard procedures. All key lock sets will meet ANSI standards to include Grade 1, mortise locksets. These requests are then forwarded to the properly annotated key/lock request form to the Security Operations Center.
5. If the request involves Fermilab taking beneficial occupancy of a portion of a new building, the requester is responsible for making notifications required.

f. Retrieving Keys from Terminated Employees

When Employment sends out electronic notice of a pending termination in FermiWorks, the employee is required to ask for a key listing of their key holdings. The employees are to bring their key list and keys to the exit interview with their HR partner. The HR partner is responsible to collect the key(s) and return them to the Security Operations Center.

When the HR partner returns the keys, the Security Operations Center employee will collect the key(s) and complete a key return in the Apex key database under the employee's key record. The key(s) will be returned to the Locksmith for destruction.

If any keys are unaccounted for, the Security Operations Center employee and/or the employee will notify Security and complete a case report. The case report number will be noted in the Apex key database under that employee's key record.

If the Security Access Specialist is notified of an after-the-fact termination, the Security Access Specialist will immediately look-up keys held by the employee. Every attempt will be made to retrieve the key(s) from the terminated employee's supervisor or HR partner.

g. Processing Miscellaneous Key Returns

If an employee returns a key, he/she no longer needs, the Security Operations Center employee will complete a Key Return in the Apex key database including the date returned. The key will be collected for destruction by the Locksmith.

h. Lost Keys

Lost keys will be reported to the Security Dispatcher and a case report initiated. The Duty Security Captain in coordination with the Locksmith, will analyze the impact of the loss and take appropriate mitigating actions. The loss report shall include an assessment of the risk involved including status of the key – unaccounted for (whereabouts unknown) or not retrievable ("fell through grate in street sewer"); does the lock provide the only level of protection to the affected space or are there other protective systems in place; value or attractiveness of the material or area being protected by the lost key. Roving security patrols are not, in this context, to be considered a redundant protective measure. The loss report should also contain a statement from the reporter as to whether all other government keys assigned to him/her are accounted for.

If the lost key controls access to a Property Protection Area, the Duty Security Captain will initiate actions to have the area re-keyed or staffed within 24 hours of the loss or being reported. The staffing will be the primary responsibility of the landlord of the space affected. Security may assist if resources permit.

i. Maintaining Records

The Apex Key Database, will contain complete records of all keys issued, returned and/or lost. The database contains all records related to the lifecycle of a key and/or core used at the laboratory, which includes key number, employee ID, and location.

j. Key Destruction

The Locksmith/Lock Shop collects all returned keys and destroys the key. Identifying information on the head of the key is separated from the key body and the key is disposed of as scrap metal.

k. Card Access (C.Cure9000)

The Security Operations Center is responsible for ensuring all Fermilab badge card holders have the required access according to their job assignments. Fermilab badges are given to those individuals who have already been properly vetted by the Foreign National Access Plan Office and Export Import Control Compliance Manager prior to the Badging Office issuing the badge. Certain buildings require authorization which may require additional training. This training complies with Fermilab Export Control requirements. The Security Operations Center and/or Deputy Physical Security Manager will ensure that the appropriate level of access is granted after reviewing the foreign national security plan for an individual, if required.

l. New Badges

Employee goes through the HR New Employee Process and gets their badge at the Badging Office. Security Operations Center provides access to General Access Areas.

Employee's Supervisor will perform an ITNA and address the specific building training safety requirements. This is based on the Employee's work location needs. Not all encompassing for access purposes. Once Training is completed, the Division Director or Building Manager (depending on location) will authorize access by sending an email to cardaccess@fnal.gov. The Security Department will identify the proximity number on the card and provide access in CCure.

m. Badge Renewals

Fermilab badge renewals are process through the badging office. All Fermilab badge renewals need to be reverified by the Manager / Access Approver. Fermilab Employees will receive the same level of access as they previously held.

Fermilab Users / Affiliates / Contractors / Authorized Guests will not receive the same level of access as they previously held. This group must be reapproved by their Point of Contact or Building Manager / Access Approver. These access approvers must give written approval through cardaccess@fnal.gov.

n. Temporary Prox Card

There are 5 Temporary Prox Access Cards that can be issued to lab personnel that forget their Fermilab ID badge at home. Security will issue a blue Business Visitor sticker at the gate to those that forget their Fermilab ID badge at home and send them to the SOC for a Temporary Prox Card. SOC must advise them to return the Temporary Prox Card at the end of their shift. The SOC will activate the temporary card so that it is active for 24 hours. The Temporary Prox Card must be returned within 24 hours of being checked out. If the card is not returned after 24 hours of being check out, then the SOC must ensure the card is disabled and call the individual to have them return the card ASAP. If all Temporary Prox Access Cards are signed out, the SOC should notify the security officers at the gates to let them know that there are no more Temporary Prox Access Cards that can be issued for the day. Security will issue a blue BV sticker at the gate and send them to their work location. If all the Temporary Prox Access Cards are signed out and someone comes to the window asking for one, please let them know the temporary cards have all been issued out for the day and make sure they have a blue Business Visitor sticker.

There are 10 Emergency Access Cards with Prox numbers that should only be used in emergency situations and issued to Law Enforcement or approved by Physical Security Manager, Deputy Physical Security Manager, or Deputy Senior Director. Each card is setup in CCure under the name: Emergency Card #1 -10. These cards already have access add to them and are good until 6/62028.

o. HR Terminating Personnel

The following activities transpire when employees terminate employment or affiliation with the laboratory.

HR will notify the Badging Office and Security Operations Center through the Fermi Works application of an imminent termination. The Security Operations Center will email the employee, the employee's manager or ITNA contact, as identified in the Emergency Call List, and the HR partner of any keys issued to the employee. The manager of the terminating employee is responsible to collect any keys and turn them in to the Security Operations Center.

p. Terminating Employee, Scheduled and Unscheduled

When an employee has scheduled his/her termination via standard employment procedures, HR sends an electronic notice of termination to the Badging Office and Security Operations Center through the Fermi Works application.

The terminating employee will be required to return or transfer all Fermilab owned property. The Security Operations Center will provide the employee with a list of keys if any, that need to be returned. Keys are uniquely stamped and are not to be passed on to other employees to keep or use. All keys must be returned to the Security Operations Center. Any property or keys that cannot be found, the employee must file a security loss report.

When an unscheduled termination occurs, HR will send an electronic notice of termination through the Fermi Works application. The HR Partner will work with the manager to coordinate the return of all Laboratory owned property.

When an employee does not report to HR for the termination process, the HR Partner will notify the employee in writing to return all access control devices. If the employee does not return the devices after a reasonable time, the Security Operations Center Supervisor will initiate a Loss of Government Property Security Report.

If an employee dies, HR will notify the SecurityDepartment. The Security Department will prepare a list of government property to include keys and Fermilab badge. The HR Partner will work with the deceased employee's family and manager in attempting to recover any

Fermilab owned property the employee may have had at his/her residence or work area. The HR Partner will notify the Security Department if any of the deceased employee's assigned property cannot be recovered after a reasonable time. The Security Department will then initiate a Loss of Government Property Security Report.

HR will notify the Security Deparment if personnel going on a leave of absence greater than 90 days will be returning government property to include keys and Fermilab badge, after consulting with that employee's supervisor.

q. Security Operations Center

When the employee reports to the Security Operations Center, the Emergency Operator/Dispatcher will receive all his/her government property to include keys and Fermilab badge, noting the date each item is received (occasionally employees elect to turn in some materials prior to their actual termination and return to complete the procedure).

The Emergency Operator/Dispatcher will sign and date the form and provide the employee with a copy for their records. If the employee cannot produce listed access control devices the Emergency Operator/Dispatcher will take the following steps:

1. Missing Vehicle Stickers - The employee's statement explaining why the sticker(s) cannot be returned should be written in the "Reason" space on the Terminating Checkout Report. The Vehicle Sticker database will be updated. The checkout procedure will not be delayed.
2. Missing Keys - If the employee states that he/she has turned any keys over to another employee, the Security Operations Center Supervisor will contact that individual and arrange for the keys to be delivered to the Security Operations Center. If the employee states that he/she has lost key(s) that have not previously been reported as lost to Security, the Security Operations Center Supervisor will instruct the employee to initiate a loss of government property security report.

r. Subcontractor Contact Representative

The Subcontractor Contact Representative will inform all subcontract personnel they are responsible for any government property to include keys and Fermilab badge issued to them. It is the property of DOE and must be returned at the conclusion of their work on Site.

The Subcontractor Contact Representative will ensure he/she collects all government property to include keys and Fermilab badge issued to subcontract personnel and return these items to the Security Operations Center when such personnel conclude their association with work at Fermilab.

The Subcontractor Contact Representative must report any items not returned to the Security Operations Center and file any required security reports.

6. Definitions

Locksmith - The full time Fermilab locksmith.

May - The use of the word "may" indicate an optional action.

Reviewing Officer - The Security Department staff person who is knowledgeable in the Laboratory's key systems and physical protection policies and is assigned by the Deputy Physical Security Manager to review all lock and key requests.

Security Access Specialist – an assigned Security Operations Dispatcher whose primary duty is to process keys, card access and site access requests on a daily basis.

Shall - The use of the word "shall" indicate a required action.

Should - The use of the word "should" indicate a recommended action.

7. Owner and Subject Matter Experts

Physical Security Manager is the owner of this procedure.

Reviewing Officer is/are responsible for reviewing, updating, and communicating changes to this procedure.

Security Operations Center Supervisor is responsible for daily oversight of the key requests, card access and site access requests.

Security Access Specialist is responsible for process daily key requests, card access and site access requests, and employee terminations for badges and keys.

Security Locksmith is responsible for processing keys, making/changing cores, and key destruction.

8. Review Cycle

This procedure shall be reviewed annually.

9. Communication Plan

This procedure will be communicated by the Security Operations Center Supervisor to all Emergency Operator/Dispatchers, and periodic training shall be provided by the Security Supervisor. Security Operations Center Supervisor is responsible for communication of this policy.

10. References

None