PART 2006 – MANAGEMENT

Subpart QQ – Rural Development Physical Security – Key Control

§ 2006.2101 General.

(a) Executive Order (EO) 12977 established the Interagency Security Committee (ISC) to enhance the quality and effectiveness of security in and protection of buildings and facilities in the United States occupied by Federal employees for nonmilitary activities (Federal facilities), and to provide a permanent body to address continuing government-wide security for Federal facilities.

(b) The ISC developed a Standard that establishes a guideline process for Physical Access Control and details access into Federal facilities and property.

(c) ISC's Standard is intended to be applied to all buildings and facilities in the United States occupied by Federal employees for nonmilitary activities. These include existing owned, to be purchased or leased facilities; stand-alone facilities; Federal campuses; individual facilities on Federal campuses; and special-use facilities.

§ 2006.2102 Authorities and References.

(a) Title 41, Code of Federal Regulations, Part 102-74, Subpart C. Conduct on Federal Property.

(b) Executive Order (EO) 12977 – Interagency Security Committee, October 19, 1995. Executive Order 13286, Amendment of Executive Orders, and Other Actions, in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security, February 28, 2003.

(c) GSA P100 Facilities Standards for the Public Buildings Service Physical Security Standards, July 2018.

(d) RD Instruction 2024-B, Identification Cards and Other Government Property Items.

(e) USDA Office of Procurement and Property Management (OPPM) Leased Space Management Handbook, March 2018.

(f) USDA OPPM Integrated Physical Security Standards and Procedures Handbook, September 2004.

§ 2006.2102 (Con.)

(g) DR 3620-001, USDA AgLearn Services, Courseware, and Content, September 9, 2019.

§ 2006.2103 Applicability and Scope.

(a) Pursuant to the authority provided to the ISC in Section 5 of Executive Order (EO) 12977, as amended by E.O. 13286, this RD Instruction identifies procedures to establish and maintain an effective key control program for each RD office.

(b) An effective access control (lock, combination, key or electronic) program minimizes the possibility of unauthorized access to a facility and assets. Possession of keys, combinations or other access control devices, represent primary authorization for an individual to enter a facility or have access to a particular asset. Possession of keys, combinations and access control cards by unauthorized individuals severely affects security and neutralizes the primary purpose of an access control program. In order to protect USDA assets, these procedures for accountability and control shall be implemented at each RD facility.

(c) These baseline procedures provide necessary guidance and assign responsibilities to each RD office, while establishing and maintaining an effective key control program. Aligning this policy with each office's overall physical security posture will help to protect property and equipment within individual offices.

(d) USDA encourages the use of an Enterprise Physical Access Control System (ePACS), or electronic / mechanical cipher locking devices. These systems greatly enhance physical security while simultaneously reducing time and overall expense.

§ 2006.2104 Applying the Standard.

(a) Physical Security is a primary supervisory obligation. The RD State Directors are responsible for appropriate physical security measures necessary to protect USDA assets. This policy establishes a baseline for key control at all RD facilities. The RD State Director may implement more restrictive key control measures based upon situations, trends, threat level, security assessments, and technology advances. RD State Directors implementing more stringent restrictive key control within a facility will notify the Director, RD Security and Emergency Management Division.

§ 2006.2104 (Con.)

(b) At a minimum, RD State Directors ensure Exhibit A, Key Control Duties, Procedures and Standards, are followed.

§§ 2006.2105 – 2006-2150 [Reserved]

Attachments: Exhibits A, B, C and D

o0o

Key Control Duties, Procedures and Standards

(A) Personnel and Duties. The RD State Director appoints, in writing, a Key Custodian (KC) and an Alternate Key Custodian (AKC) for each facility in the State. These individuals are duty-stationed at the assigned facilities. In the KC absence, the alternate assumes all duties related to key control. For buildings under the operational control of the National Office (USDA South Building, USDA St. Louis), the Chief Operating Officer (COO) will delegate appointment responsibility to on-site leadership within the Enterprise Office.

(B) Key Custodian. The Key Custodian (KC) is responsible for the operation and general function of the office lock and key control program. Overall, the KC is directly responsible for identifying, receiving, issuing, categorizing, marking, securing and safeguarding all access control devices (keys, combinations, key cards, key-fobs, RF tags, etc.) used to gain access to all RD space, buildings, containers, and vehicles. Specific duties include:

(1) Determining the location and category of all locks at a facility.

(2) Determining the operating status of all locks and keys in use. This includes identifying damaged, lost, missing, stolen, or inoperable locks, keys, combinations, key cards, etc. Lost, stolen, or misplaced keys will be reported, in writing, to the RD State Director. The affected locks will be rekeyed or replaced. Misplaced or compromised combinations will be changed immediately.

(3) Arranging a key repository, including selecting storage containers, key rings, and key tags. Safeguard all keys in a lockable, steel type key repository affixed to a wall or in a container that is not easily movable.

(4) Identify, where feasible, all keys by engraving “US GOVT DO NOT DUPLICATE”.

(5) Serializing (engraving, marking, labeling, etc.). In instances where no serial number (SN) exists, the KC will assign each lock and corresponding access device an individual alpha-numeric identification.

(6) Prepare an administrative memorandum access roster detailing who has access to the key repository during KC absence. This access roster shall be protected from view from those without a legitimate need to know.

(7) Combinations are changed when individuals depart the organization, or at a minimum on a quarterly basis, safely disseminated, secured, and updated properly. Areas with multiple combination locks will be assigned combinations which are not duplicated or easily guessed, e.g., street number, zip code, telephone numbers, etc.

(8) Maintain a Key Inventory Log for the identification of keys and corresponding locks; Key Control Log documenting to whom keys were issued and received from; and a Key Issue Record to document receipt of issued keys and acknowledgement of key holder responsibilities. See samples of each at Exhibits B, C and D, respectively.

(9) Conducting periodic inventory of all keys and locks. Locks and corresponding access devices shall be inventoried annually with exception to facility entrance/exit doors, and sensitive infrastructure rooms (IT/computer/ADP, etc.) which shall be inventoried quarterly. A written record of the inventory will be prepared and filed in accordance with record storage directives. Minimally, these files will remain for three years. These files are subject to review during physical security assessments.

(10) Ensure key duplicates are kept to a minimum.

(11) Limit the issuance of keys to employees and authorized contractors who have a legitimate need for unaccompanied access.

(12) Combinations shall be changed as soon as feasible when an employee or contractor, who was issued the combination, no longer requires access (retirement, transfer, termination, end of contract, or other extended absence).

(13) Access devices and combinations shall not be provided to any personnel who have not undergone a successful background investigation.

(14) Locations possessing critical infrastructure, keyed without the benefit of electronic access controls, should consider re-keying each lockset at least annually. Offices are highly encouraged to procure and install cipher locks for usage in these instances.

(15) Offices possessing significant quantities of access control devices should consider a computerized key management database to aid with key inventory.

(C) Alternate Key Custodian. In the absence of the KC, the Alternate Key Custodian (AKC) is responsible for the operation and general function of the office lock and key control program. The Facility Security Committee may appoint more than one AKC in facilities that are represented by the FSC when more than one USDA organization shares space. A strong working relationship with State Directors and FSC is required.

(D) Key Control Training. Designated key control program personnel shall be formally trained in lock and key control procedures and responsibilities using initial and periodic sustainment opportunities. Training should be comprehensive and provide a strategic understanding of how lock and key control can affect the security of a federal office. Minimally, training should include the following topics:

(1) How to minimize the risk of a lock compromise.

(2) Lock maintenance requirements.

(3) Lock and key control procedures.

(4) What to do in case of a lockout.

(5) Proper key security, including procedures for dealing with lost, missing, stolen, or damaged keys.

(E) Training programs should be designed to hold the attention of attendees. Use examples and scenarios that describe real situations and problems (e.g., thefts that have taken place or careless acts that can compromise a key control program). Diagrams, videos, pictures, or charts can be used to illustrate the subject and make the training more interesting. Regardless of the method, training of employees is essential to a successful lock and key control program.

(F) All training will be tracked in AgLearn in accordance with DR 3620-001, USDA AgLearn Services, Courseware, and Content, September 9, 2019.

o0o

Sample Key Inventory Log (usable PDF/Excel available on SEMD Share Point)
RD Key Inventory

RD KEY INVENTORY - *EXAMPLE*			
Room #	**# of Keys**	**RD Organization**	**Notes**

o0o

Sample Key Control Log (usable PDF/Excel available on SEMD Share Point)
Key Control Log

RD KEY CONTROL LOG

Room Number	Name	RD Organization	Number of Keys Provided	Signature	Date	Key(s) Distributed By

o0o

Sample Key Receipt Checklist (usable PDF/Excel available on SEMD Share Point)
Key Receipt Checklist

Rural Development - Key Receipt Checklist			
Date			
Key Issued To		Supervisor Name	
Building		Room Number	
Statement of Acknowledgement of Receipt of Key			
I understand that keys issued to me provide access to the space listed above. Additionally, I have read and am familiar with the Key Control Policy. I understand the following provisions apply:			
a. Keys are property of the U.S. Government. b. Upon my departure (transfer, reassignment, retirement, resignation, or removal), the keys must be returned to the Key Custodian (as identified in the Key Control Policy). c. Any loss or damage of keys must be reported to the Key Custodian immediately. d. It is my responsibility to ensure that all spaces to which I have keys are locked at the end of my business day. e. Keys must remain in my possession at all times. Loaning or duplication of key(s) is strictly prohibited. Failure to comply may result in disciplinary action. Key(s) shall remain in the possession of the assigned holder at all times. Any person giving possession of their assigned key(s) to someone else could result in disciplinary action up to and/or including termination.			
Employee Signature			
Key Custodian Signature			

o0o