FEDERAL AVIATION ADMINISTRATION
Mike Monroney Aeronautical Center
Office of Facility Management

ORDER
AC 1600.85

Effective Date:
06/01/2020

SUBJECT: MMAC Key Control Policy

1. Purpose of This Order. This Order establishes and prescribes key control procedures at the Mike Monroney Aeronautical Center (MMAC) to help protect the life, property, and security of the MMAC and all its occupants.

a. It must serve as the framework by which all keys and access credentials will be managed, issued, duplicated, stored, controlled, returned, replaced, and accounted for by the Operations and Maintenance Division (AMP-300) Key Control Official (KCO).

b. This policy must apply to all keys (physical and electronic) including those to all space, office equipment, padlocks, lockers, safes, etc., owned, operated, or controlled by the Facility.

c. This policy seeks to establish a recorded chain of accountability and access for all credentials, key holders, and locations.

(1) Establish a key issuance authority.
(2) Issue appropriate level keys to individuals.
(3) Establish authority on all key control policies.

d. This policy seeks to implement a proper key control process and then preserve it by restoring security in a timely manner whenever key control has been threatened or compromised.

2. Audience. All Federal Aviation Administration employees, contractors, and tenants residing at the MMAC who manage key control procedures and/or are issued keys to Center facilities.

3. Where You Can Find This Order. The published Order is located on the FAA.GOV website at https://www.faa.gov/regulations_policies/orders_notices/ or on the MyFAA Employee website at http://www.faa.gov/regulations_policies/orders_notices.

4. Related Publications and References. See Appendix B, AC 1600.21xx

5. Definitions. See Appendix C, AC 1600.21xx

6. Explanation of Policy Changes.

a. Establishes a separate policy under Order AC 1600.21xx for key control.
b. Updates the key control procedures for MMAC.
c. Revises Roles and Responsibilities to reflect new policies and procedures for key control at MMAC.
d. Provides required policies and procedures for issuing keys to employees, contractors, and tenants residing at the MMAC.

7. Background. In support of the FAA's continuing mission to provide the safest, most efficient aerospace system in the world, the MMAC promotes academic and industry partnerships and has a keen interest in international cooperation in the research, development, and acquisition of aviation systems and technologies that enhance aviation safety. These efforts involve official and unofficial visits by a wide range of people including U.S. persons (i.e., U.S. citizens and U.S. nationals), foreign nationals, and foreign representatives.

8. Scope. This Order must be distributed to program director level at the Aeronautical Center and to all tenant heads.

9. Roles and Responsibilities.

a. AMP-300:

(1) Responsible for managing key control procedures within all areas, buildings, and facilities.
(2) Approved authority for issuance of keys to MMAC areas, buildings, and facilities.
(3) Provide Key Control Official

b. Managers, Supervisors and Contracting Officer's Representatives (COR):

(1) Ensure only those individuals that require access to secured/restricted areas are issued keys.
(2) Ensure retrieval of keys from employees that no longer require access, have transferred to another organization, or no longer work at the Center.
(3) Request installation/removal of locks from areas, buildings, and facilities within their area of responsibility.
(4) Only request keys to areas established under their authority.
(5) Only request keys necessary to perform job functions.
(6) Ensure all keys are returned to the Locksmith (Pass and ID) upon a key holder's separation, termination, or retirement from the Center.
(7) Conducts annual inventory of all keys issued to personnel assigned to their areas of responsibility, to include employees and contractor personnel, unless otherwise directed by the Facility Manager. Facility Manager is accountable for annual inventory during AXF inspection.

c. Key Holders:

(1) Ensure that all master keys, sub-master keys, and keys not required for access to office/work remain on MMAC and are secured (see paragraph 13c).
(2) Ensure keys that are no longer required for authorized purposes are returned to the Key Control Official within Facility Management.
(3) Do not alter, duplicate, copy, or make a facsimile of any key to a lock of an MMAC building or property without receiving written permission from the Key Control Official who will maintain a copy within Facility Management.
(4) Use assigned keys for access to authorized locks only.
(5) Take measures to protect and safeguard any keys received.
(6) Do not loan keys to other individuals.
(7) Immediately report damaged keys or locks to AMP-300.
(8) Ensure all unlocked doors/locks are secured afterhours access and that doors are not propped open.
(9) Ensure that keys are not stored in desk drawers or in other unsecured areas.
(10) Immediately report any lost, missing or stolen keys or locks to the SSE via the WebIRS applications (https://incidentreporting.faa.gov/)

d. Key Control Official. The MMAC Key Control Official and alternate(s) must be responsible for ensuring the following:

(1) An adequate supply of key blanks and electronic key cards are maintained on hand for required use.
(2) Spare keys, locks, and key codes are properly secured.
(3) Required key records are maintained.
(4) Ensures responsible Managers / Authorizing Officials conduct annual inventory of keys, unless otherwise directed by the Facility Manager.
(5) Conduct annual inventory of keys not issued.
(6) Ensure all lost keys and electronic access cards are reported to the SSE by way of the WebIRS reporting application.
(7) Overall supervision of the key program.
(8) Ensure the quantity of keys, electronic access cards, or combinations is kept to a minimum and issued only to persons who need them for official duties. Only the KCO or alternate may issue keys, electronic access cards, or combinations.
(9) Ensure unissued keys and cores that are not in use are stored in an approved locked container. Access to this container will be limited to the KCO, alternate KCO, and Facility Manager (FM).
(10) Determine in coordination with the SSE and the FM the extent to which locks must be re-cored, changed, or otherwise modified to prevent compromise of existing safeguards. Generally, the loss of any grand master key, or any two sub-master keys, the control key or five percent of the keys of a series is considered to have compromised the whole series.
(11) Physical Access Control System (PACS) Review. The Facility Manager or their designee(s) must review the personnel access privileges permitted by the system quarterly. Data reviewed must be extracted from the PACS for each cycle to ensure

accuracy. At least once per year, this must be done by the Facility Manager, not a designee. A thorough PACS review will also be conducted upon change of FM responsibilities.
(12) Annual Review. The Facility Manager or their designee(s) will change and document all alarm arming/disarming codes and combinations. Annual inventory of all keys, cores, and electronic access cards by the Key Control Officer (KCO).

10. Special Precautions. Security containers used for the storage of keys, cores, and electronic access cards must be protected from public view and have restricted access.

11. General. The MMAC standard locking system is the system manufactured by the Best Access Systems. The standard key inventory and management system is the Archibus system. The systems include the cores, keys, locksets, padlocks, and codes for a proprietary system.

a. Acquisition of Locks, Keys, Cores, and Codes. This includes the acquisition of all hardware (locksets, padlocks, etc.), cores, keys, codes, electronic locking/unlocking systems, card access systems and cards, cipher locking systems, etc. This also includes the knobs, spindles, case, trim, etc. Deviation to the FAA locking systems for use at the MMAC may be approved by ASH to support research and development, to comply with security directives, or to meet unique security requirements.

b. Change of Locks/Cores within a Locking System. Requests for lock or core changes within an organization's locking system must be submitted directly to the MMAC Key Control Official (AMP-300). This includes replacing defective cores, changing locations of cores, adding or deleting cores, etc. Requests must be authorized at the division level or higher.

12. Procedures. All organizational keys and locks will be stringently controlled and accounted for at all times. Control measures for sensitive items and medical or classified items as described in other regulations have precedence. In the absence of guidelines elsewhere, the minimum standard measures described herein are to be applied in every case.

Specific procedures include:

a. Requests for keys must be submitted in Archibus to the Key Control Official (AMP-300) by the manager responsible for the area secured by the door or the COR for the applicable contract via the Archibus Space POC for each organization.

b. Requestor will be notified when request is approve/disapproved.

c. Keys must be picked up from the Locksmith at the Security Command Center.

d. Only approved persons can sign and take custody of the key(s).

e. Keys not picked up within thirty (30) days of the approved requested will be returned to storage or destroyed.

f. Key(s) must be returned to the Locksmith when no longer needed. Keys are not transferable and must be accounted for before final employee clearance is granted.

g. Only those keys required by organizational personnel to gain access to individual work areas and buildings will be signed out for personal retention.

h. Specific keys used to secure Government property that is accessible only to authorized individuals will remain locked in the organization key depository and properly signed out as needed to authorize personnel.

i. Combinations to safe locks will be strictly controlled and protected to prevent loss or compromise. Specific procedures are as follows:

(1) Combinations will be recorded on SF 700 (Security Container Information). The information copy of the form will be posted inside the container (safe, file cabinet, etc.) out of direct view whenever the container is open. Additional procedures for protection of combinations for containers or safes storing classified information will be followed and are contained in FAA Order 1600.2 and FAA Order 1600.8.

(2) Combinations will be changed annually, when compromise of the combination has occurred, or whenever an individual with access to the container is no longer assigned to the activity.

(3) A record copy of the SF 700 will be sealed in an envelope. The sealed envelope containing combinations will be secured with the key control custodian or with the Servicing Security Element (SSE), if the safe contains classified information.

h. Master keys are not authorized unless approved by the Facility Manager.

i. Individually owned locks will not be used to secure or protect Government property.

j. Individually owned locks and keys used to protect or secure personal property are excluded from key control procedures.

13. Administrative Controls.

a. The number of personnel authorized to possess (personally retained keys) and use keys will be limited to those persons who have an absolute need, as determined by the supervisor responsible for the activity.

b. Keys for offices, entrances to buildings, and individual rooms may be issued for personal retention. Keys for maintenance buildings, supply buildings and rooms, and property storage areas may be secured in an approved depository after duty hours or in the custody of the Contract Security Officer. Keys will be secured separately from all other items.

c. All keys when not in use will be secured on the person of the individual to whom assigned or secured in a lockable container such as a safe, filing cabinet, or key depository made of at least 26-gauge steel that is equipped with an approved 5-pin tumbler locking device or combination lock or padlock. Keys must not be left in the key-way of the locking device or in any fashion so as to permit easy access from unauthorized use. Key depositories or containers that are easily removed will be securely affixed to the structure. The key depository will be located in a room where it is kept under surveillance around-the-clock or in a room that can be securely locked during nonduty hours.

d. Portable key containers will be secured, when not in use, in locked steel cabinets or other approved containers. Other methods for securing portable key containers must be approved in writing by the Key Control Official. Requests for approval should be made on a standard memorandum which describes the container, the procedures in use, and the reasons for exception.

14. Accountability Procedures.

a. Audits:

(1) Key System:

- Under normal circumstances, all keys and cylinders will be evaluated for change at intervals not exceeding five (5) years.
- Reports must be periodically generated and distributed by department with a written response required to confirm the accuracy of the information being held.
- Master inventory. All keys to locking devices used to secure or protect Government property will be strictly accounted for at all times. A complete written inventory of all keys will be maintained by the Key Control Official.
- Daily inventory. A daily 100 percent visual count of all primary keys (those operational keys secured in the daily use key box or depository) will be conducted by the individual authorized to receive or issue keys at the start of each duty day. Discrepancies between the closing and opening inventory counts will be investigated and resolved before issuing any keys.
- Annual inventory. Once each year a 100% inventory of all keys in the system will be conducted by the responsible manager/authorizing official. Personally retained keys will be provided during each inventory for accountability and inspection. Each key on the last inventory must be accounted for either by being issued, returned or have a loss (incident) report on file. This inventory will coincide with the Key Control Officials inventory, which accounts for all keys not issued and in the key container or keys that have a record of destruction.

b. Issuance and Return of Keys.

(1) Government Employees. Keys are issued to FAA employees to access buildings, work areas, restricted areas, and closed areas. All of these types of keys are “security keys.” Security keys are used to protect U.S. Government employees, information, and

assets. Security keys may not be issued to all employees. The criterion for issuance of a security key is the need to gain access to a specific area to perform official duties. Convenience, position, or an occasional need for access may not be used as the sole basis for issuance of a security key. Since the issuance of keys (including metal keys and key cards) is critical to the value of a locking system, each office director/staff manager and tenant division / group manager must be responsible for ensuring keys are issued to the employees under their control only on the basis of valid need.

- Keys must be returned to the Government upon request of the authorizing official, when changing jobs or organizations, clearing the facility, retiring or terminating, or whenever the official need for the key no longer exists (for example, a change in job function, extended military leave, extended sick leave, suspension for cause, etc.).
- If an employee is suspended for cause, it will be the responsibility of the employee's manager and/or supervisor to retrieve the employee's keys and access cards. Those keys/access cards will be returned immediately to the MMAC Locksmith.
- Keys are issued to individuals only and not to offices or organizations. Keys must not be loaned or borrowed. Archibus key requests must be in a standard format and must contain the following information at a minimum, Name, routing symbol, and telephone number, signature of the key holder, building and room number for the key and signature of the authorizing official.
- If a master or sub-master key is being requested, Archibus must contain the justification why the master or sub-master key is required rather than a normal security key.
- Only a division manager or program director can request the issuance of a master or sub-master key.
- Signature of concurrence from the responsible official's area/facility to be accessed if different from the key holder's organization.
- Acting managers are authorized to sign applications for keys only if they have been officially detailed into the position with an SF-50 for a period exceeding 30 days.

(2) Contractors. The criteria for the issuance and return of keys to contractors must be the same as for Government employees with the following exceptions:

- Their contract states that the contractor will abide by FAA Orders and Policies concerning the protection of Government property from loss, theft, or vandalism.
- Their contract provides for the issuance of keys, withholding for the loss of keys, and requires the contractor to provide a personnel security background investigation for each person to whom a key will be issued.
- Keys and access cards are Government property and must be controlled just as any other type of accountable Government property by the Contracting Officer (CO) or the COR.

- The CO or COR is responsible for immediately notifying ASH and the MMAC Key Control Official (AMP-300) of the loss or theft of any keys or access cards issued to a contractor.
- The CO is responsible for initiating procedures for the appropriate withholding from the contract payment if required. All Archibus key requests must be in a standard format and must contain the following information at a minimum, name of the contractor, routing symbol, telephone number of COR justification statement must include that the key is issued directly to a contractor, building and room number for the key and signature of the authorizing official.

(3) Procedures for Issuance of Electronic Access.

- Application for electronic access to the flight line, logistics facilities, computer rooms, etc. Applications for electronic access to the flight line must be coordinated with and include signature approval by the Flight Program Operations Division.
- Application for electronic access to logistics facilities (Logistics Support Facility (LSF), Technical Support Facility (TSF), or Thomas Road Warehouse (TRW) must be coordinated with the Logistics Security Specialist (AML) and have signature approval on the application.
- Application for electronic access to the SMF computer room(s) must be coordinated with, and have signature approval on the application, by the Program and Resource Management Division in the Enterprise Service Center (ESC).
- Applications for electronic access for all other areas must identify the days and hours that access is required (i.e., Monday through Friday, from 6 a.m. to 6 p.m.) If the status level is known, it should also be specified. Electronic cards other than PIVs assigned to FAA employees that are broken or damaged must be returned to the Center's Pass and ID office, located in the Security Command Center (Building 230), for replacement. Electronic cards assigned to contract employees that are broken or damaged must be returned to the CO or the COR for replacement. A new application is not required for the replacement of a broken or worn card.
- Facility Management will terminate access upon notification of a violation or upon LOB management request or notification.

****Note: This section does not apply to the issuance or replacement of the PIV. The replacement/issuance of a PIV is through the HSPD-12 / PIV Desk, located in Bldg. 230.****

15. Identifying Keys and Keying

a. All keys should only be marked with a blind code number that does not in any way reflect its usage or level.

b. The use of standard key coding to mark cylinders or keys is not authorized.

c. New sub-masters and master keys will not be marked SM or M to indicate level of keying.

d. All new issued keys will contain an inventory or serial number that reflects the total number of keys issued and provides a unique identifier for every copy.

e. Keys must not be stamped with bittings.

16. Non-returned Key Policy

a. A cost replacement fee for lost or stolen keys may be charged to the key holder's organization; if it is determined, the key was lost or stolen due to key holder negligence or failure to follow the procedures established in this policy.

b. Re-keying charges may be charged to the organization, department, individual, or company responsible for losing the key. Rekeying charges must be determined by the number of locks operated by the lost or stolen key(s).

c. If any individual has two or more separate incidents of lost, stolen, or non-returned key violations within a one (1) year period, key privileges may be revoked.

17. Storage.

a. Keys, credentials, and key records must be stored in a secure condition (data) or location (physical items) protected by lock and key or vault.

b. Keys must be stored in a locked cabinet or container in a secured area.

c. Key rings issued for temporary use must be of a tamper resistant design so that keys cannot be removed from the ring prior to return.

d. Emergency key storage boxes (Knox, Supra type): Subject to local regulations and to protect against theft or duplication, no master keys should be stored in these types of containers.

e. Key records must be stored in a secure location that is protected against both fire and theft:

(1) Bitting lists.
(2) Authorization forms.
(3) Key issuance and return records.
(4) Data files must be password protected and encrypted.

18. Key Management Format. The key management system must be maintained in a computerized format. The MMAC Key Control Official must be responsible for maintaining records; tracking the total number of keys and cores by number; keys by name of key holder; locks by lock number; lost keys by key number; lost key reports; and electronic access card inventories and transactions. These records must show at a minimum the following:

a. A listing of all cores by those currently installed in the facility and their locations, those in storage, those destroyed, and those lost or stolen.

b. A listing of issued keys, locks, and electronic access cards by series number and/or serial number (as applicable) showing whom they were issued to and the date they were issued. The listing will include each individual's access privileges for electronic access cards. Keys must be issued using a form that bears the recipient's signature and has a responsibility statement on it such as the FAA Form 4650-11, Memorandum Receipt.

c. A listing of non-issued keys, locks, and electronic access cards by series or serial number (as applicable).

d. A record of all keys not accounted for. Include whom the key was last issued to or the last known location of the core, when it was last accounted for, and when the loss was reported to ASH.

e. A listing of destroyed keys, locks, or electronic access cards

f. A listing of combination locks by door number, location, and the date of the last combination change

g. Any other documentation to include: purchase orders, hand receipts, evidence of baseline acquisition, etc.

19. Record Keeping

a. All key records must be kept current at all times and are to be considered Controlled Unclassified (CUI).

b. Any hardcopy Records must be securely stored

c. All transactions must be recorded in a timely manner

20. Servicing

a. Cutting keys:

(1) Only the Center-approved locksmith must be permitted to cut keys.
(2) All facility keys must be cut on factory approved code cutting machines, not on duplicating machines that trace from one key to another.

b. Pinning/re-combinating cylinders:

(1) Must only be performed by an MMAC approved locksmith.
(2) Must be on the MMAC's key system unless approved by the Facility Manager.

(3) Combinate to all appropriate levels of keying unless pre-approved by the SSE.

c. Installing locks:

(1) Must only be performed by an MMAC approved locksmith department.
(2) Must be on MMAC's key system unless approved.

d. Preventative maintenance must be performed regularly to ensure proper operation of keys and locks and to maintain security.

(1) Worn keys must be replaced to avoid breakage.
(2) Worn or poorly functioning cylinders must be replaced to maintain proper security.
(3) Key cutting machines must be checked and calibrated regularly, IAW the manufactures maintenance schedule or at least annually.

e. Locksmithing work must only be performed by:

(1) MMAC Security Contract Locksmith assigned to the Pass and ID section as defined by the Performance Work Statement (PWS)
(2) Contractor locksmith business as approved by AMP-300.

21. Key Request Form

The official key request form AC 1600-6xx can be found on the FAA website in the following location:

https://employees.faa.gov/documentLibrary/media/Form/AC_Form_1600-6_Key_Electronic_Access_Request.pdf

This form must be submitted with the Archibus key request.

Kevin Gerard O'Connor
Digitally signed by Kevin Gerard O'Connor
Date: 2020.08.05 16:51:12 -05'00'

Kevin O'Connor for
Michelle Coppedge
Director, Aeronautical Center, AMC-1