

STANDARD OPERATING PROCEDURE KEY AND LOCK CONTROL

PURPOSE: To establish procedures and provide guidance for Isles District schools' key and lock control programs.

REFERENCE: DoDEA Regulation 4700.2, *Department of Defense Education Activity Internal Physical Security*, 27 March 2001

RESPONSIBILITY: All Isles District assigned personnel must ensure compliance with this Standard Operating Procedure (SOP). School principals have the direct responsibility to ensure compliance for their respective schools. It also applies to the Isles District School Bus Offices. Applicability to contractors is implied through contractual agreement to adhere to security policies and procedures established by the U.S. Government and its agents.

PROCEDURES:

1. Property Protection

1.1. All DoDDS employees and contractors shall provide reasonable care to protect government property issued to them or located within their workplace. This includes accountable property, furniture, vehicles, and expendable supplies. Reasonable care is defined as actions a responsible person takes to prevent property from being damaged, stolen, or abused.

1.2. Each person shall ensure his or her office and/or classroom is properly locked at the end of the duty day. When more than one person shares an office or classroom, the supervisor of that activity shall establish procedures to ensure one of the occupants is responsible for locking the office. Small, easily pilfered items, such as calculators, cellular telephones, cameras, etc. shall be placed in desks, filing cabinets or closets when not in use. Sensitive files shall always be stored in locking cabinets. Classified documents shall always be stored in an approved storage container described in DoD 5200.1-R, Information Security Program.

1.3. The local security office (Air Force Security Forces, Naval Security Forces, Ministry of Defence Police, etc.) conducts routine checks of buildings. When buildings are found insecure, the local security forces patrol enters the incident in his or her log and notifies the responsible building custodian or principal through their respective notification process. The building custodian or principal shall ensure appropriate corrective actions are taken as directed by local host military or MoD security officials to ensure proper security of DoDDS facilities and property.

2. Key Control. Each school as well as the Isles District office will have Key Control Officers appointed in writing.

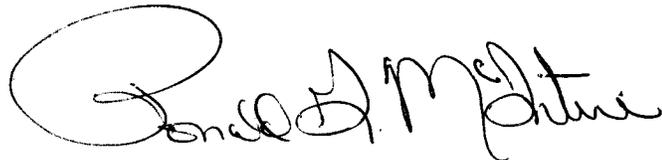
2.1. The Key Control Officer for each facility issues only those keys that are required to perform each employee's duties. The recipient is responsible for ensuring those keys are protected from loss, theft or duplication with the same degree of protection a person normally gives to protecting keys to their home or automobile. Master keys are strictly controlled and shall not be issued to persons unless their routine duties specifically require use of a master key.

2.2. Special projects such as LAN installation/maintenance, carpet shampooing, etc. occasionally require technicians or custodians to have access to offices during non-duty hours. The facility Key Control Officer shall issue keys to these individuals sparingly in accordance with requirements delineated in the contract or for the duration of a special project, as appropriate. If possible, provide supervision by an employee or staff member either by continuous supervision or by spot-checking the work area.

2.3. Key Control Officers will issue, control, and inventory keys according to procedures in DoDEA Regulation 4700.2, Enclosure 3 (see Attachment 1).

2.4. Individuals on extended periods of leave (annual leave, sick leave, leave without pay, summer vacation, etc.) should return their keys to the appropriate Key Control Officer for safekeeping. This reduces the amount of keys circulating during down time, reduces key loss, and enables the key control officer to conduct a physical inventory during the summer months.

2.5. Each Key Control Officer is responsible for writing and maintaining a Key Control Annex as described in the attachment.

A handwritten signature in black ink, appearing to read "Ronald G. McIntire". The signature is written in a cursive style with a large, looping initial "R".

DR. RONALD G. MCINTIRE
Superintendent

Attachment:
DoDEA Regulation 4700.2, Enclosure 3

E3. ENCLOSURE 3
KEY AND LOCK CONTROL

E3.1. KEY AND LOCK CONTROL

E3.1.1. A key and lock control system encompassing all locks and keys used to secure U.S. Government property will be established for all the DoDEA activities. In designing the system, planners must be cognizant of the fact that locks are only delay devices. Their adequacy and effectiveness are only as good as the controls placed over the keys or combinations to open them. A key control system supplements other security measures used to control access to schools, facilities, and offices. This control system is essential for the proper protection of facilities, and the equipment and material contained therein.

E3.1.2. Keys to administrative offices, classrooms, storage areas, desks, storage lockers, etc., should be included in the internal security key and lock control system.

E3.1.3. The DoDEA activities that are tenants on U.S. Government installations or tenants in Government-owned or privately owned buildings will comply with the provisions of this section to the maximum extent possible, commensurate with the existing lease arrangements, security support agreements, and/or memoranda of understanding.

E3.1.4. The office manager or school principal is ultimately responsible for all key and lock controls for each respective activity. However, a staff member may be designated in writing as key control officer (may also be known as the key custodian) responsible for the daily operation of the key and lock control system. The designee will be responsible for the overall supervision of the key and lock control program, the supply of locks and how they are stored, the issuance and handling of keys, records maintenance, investigation of lost keys, and maintenance and operation of key repositories.

E3.1.5. Depending upon the size of the school or activity, a key and lock control system may consist of a single system or a number of subsystems. Each system and subsystem will have a designated key control officer and a key repository.

NOTE: Equivalent key and lock control systems (such as modified automated or hardcopy systems) other than outlined here are authorized but must be individually approved for use by the District Safety and Security Officer. Equivalent control systems must meet the intent and control afforded by the controls outlined in this Regulation. Mechanical card access systems using magnetic coding has also proven to be very durable, manageable, and cost effective at the school level as the need for rekeying is drastically reduced or eliminated. However, product availability and maintenance support varies from area to area, so research should be conducted prior to commitment to nontraditional locking systems.

E3.1.6. The District Safety and Security Officer shall review the key and lock control system and will accomplish the following:

E3.1.6.1.1. Advise the principal and the key control officer on all matters relating to lock and key control systems.

E3.1.6.2.1. Inspect the implemented systems during scheduled school visits. Evaluate any key and lock control systems other than those provided here for adequacy.

NOTE: Automated control systems must be password controlled, routinely backed up to controlled disks, and may not be resident on networked drives.

E3.1.6.3.1. Ensure that external locking devices are checked during non-duty hours by installation security personnel and that a contact person is identified to receive reports of violations, tampering, or illegal entry.

E3.1.7. DS Form 4701, Key Repository Index, or its equivalent, will be maintained for each repository within the key and lock system. The index will be kept inside the repository, or under equivalent safeguards, and will be used as a basis for inventories of keys controlled from the repository.

E3.1.8. Distribution of master and sub-master keys must be strictly controlled. A useful guide in determining this distribution is to issue master and sub-master keys only to those persons that would be routinely expected to respond during non-duty hours for emergency access to multiple offices or school areas. After this careful and considered distribution of keys, all keys within the key and lock system must be accounted for at all times. This will be accomplished as follows:

E3.1.8.1. The key repository will be located in a secure room, preferably the principal's or assistant principal's office, out of sight of casual visitors and not accessible to staff.

E3.1.8.2. DS Form 4702, Key Repository Accountability Record, or its equivalent, will be used to maintain accountability of each repository and the keys contained therein.

E3.1.8.2.1 If an individual signs out the repository key from the key control officer, an inventory of keys contained therein will be accomplished, using DS Form 4702, or its equivalent. This individual will then complete the DS Form 4702, or its equivalent, leaving the block titled "SIGNATURE OF INDIVIDUAL RELIEVED OF RESPONSIBILITY" blank. The "REMARKS" block will be annotated, "Opening Inventory." On return of the repository key, the procedure will be reversed. The block titled "PRINTED NAME AND SIGNATURE OF INDIVIDUAL ASSUMING RESPONSIBILITY" will be left blank and the "REMARKS" block will be annotated "CLOSING INVENTORY."

E3.1.8.2.2 Discrepancies detected during repository inventories will be annotated in the “REMARKS” block of the DS Form 4702, or its equivalent, and will be reported immediately to the school key control officer.

E3.1.8.3. DS Form 4703, Key Control Register, or its equivalent, will be used by the key control officer to record the issue and turn-in of keys. A separate, up to date, DS Form 4703, or its equivalent will be locked inside the repository to which it pertains. All keys - removed from, or returned to, the repository will be recorded on both copies of the Key Control Register.

E3.1.9. Keys normally issued and used as a group will be affixed together, as a set, on metal rings. Each ring will include a metal or plastic tag stamped or imprinted with a ring identification code. Rings may be signed out by the identification code. However, the serial numbers of each key on the ring must be identified in the Key Repository Index, DS Form 470 1, or its equivalent.

E3.1.10. All keys and padlocks within the key and lock control system, to include keys issued for personal retention, will be inventoried by serial number annually. A record of the inventory will be maintained by the key control officer until completion of the next scheduled inventory. Individuals or groups issued keys should be advised that government keys may not be duplicated.

E3.1.11. Padlocks in use within the key and lock control system will be rotated once every 12 months.

E3.1.12. Under no circumstances will a lock be left hanging open on a hasp, staple, hook, or other device. In all cases, locks will be relocked to the locking device immediately after opening, and the key will be removed. This action prevents surreptitious substitution of locks. Keys should not be issued to personnel employed by organizations other than the DoDEA for personal retention except in extenuating circumstances and under a memorandum of understanding delineating responsibilities for care of the U.S. Government property and facilities. Under no circumstances should non-DoDEA personnel be issued keys to controlled areas; e.g., computer rooms, media storage, principal’s office, etc. Custodial service personnel should clean controlled areas prior to departure of the principal or responsible school/activity personnel.

E3.2. KEY CONTROL ANNEX. Since each school or facility will have conditions and requirements peculiar to its activity, key control systems will vary. Before establishing a system, a survey should be conducted to determine actual requirements and to identify all classrooms, storage areas, safes, tiling cabinets, etc., that require the additional protection afforded by locking devices and security of keys. When this determination is made, an annex to the physical security plan or standard operating procedures shall be prepared which shows the following information:

E3.2.1. Location of key repositories.

E3.2.2. Keys (by building, area, or cabinet number) to be turned in to each repository.

E3.2.3. Method of marking or tagging keys for identification.

E3.2.4. Method of control of issue and receipt of keys, and identification of personnel authorized possession of keys.

E3.2.5. Action required if keys are lost, stolen, or misplaced.

E3.2.6. Frequency and method of lock rotation.

E3.2.7. Assignment of responsibilities by job or position title.

E3.2.8. Emergency type keys, which would be readily available to the installation security officer, district security coordinator, or area service center security officer.

E3.2.9. Other controls deemed necessary to facilitate the effectiveness of this particular key and lock control system.