The Key/Electronic Access Control Guideline is used to address control of facility keys and keyless electronic codes used for employee access to site facilities. This guideline is also used when facility owners have delegated entry via keys/electronic entry to TFS.

**Key Control**

1. The senior-level employee at each office location is responsible for designating a budgeted employee to serve as key coordinator for the location.
2. Each request for keys is approved by the senior-level employee to ensure that keys are issued for only the necessary level of access.
3. The employee picks up the assigned keys from the key coordinator.
4. The key coordinator fills out the necessary information on the [Key Control Log](http://tfsfinance.tamu.edu/modules/finance/admin/guidelines/Key%20Control%20Log.docx). The employee signs and dates the log when keys are issued to and returned by them.
5. Unissued keys are maintained in a locked cabinet or drawer for security purposes. Access to the locked cabinet or drawer should be limited to the key coordinator and the senior-level employee.
6. When an employee terminates or transfers, their supervisor is responsible for verifying that the keys have been returned to the key coordinator before signing off on the Employee Out-processing Checklist.
7. The key coordinator should maintain an accurate inventory of keys to buildings, gates, etc.

**Keyless Access Code Control**

1. The senior-level employee at each office location is responsible for designating a budgeted employee to serve as electronic access code coordinator for the location.
2. When electronic locks are installed on facility doors, the factory default code should be changed before providing the code to employees that require access.
	1. Avoid using personally identifiable information as the access code. Numbers to avoid are things like street address, P.O. Box number, birthdays, phone number and ZIP code.
	2. Don’t choose numbers that are in consecutive order, even if they’re reversed or in a set pattern on the key pad.
3. Each request for the access code is approved by the senior-level employee to ensure electronic access is limited to employees that require access.
4. Employees receive the access code from the electronic entry coordinator. Employees should protect access codes in the same manner that they would a key.
5. The electronic access code coordinator documents the name of each employee granted electronic access on the [Electronic Access Code Control Log](http://tfsfinance.tamu.edu/modules/finance/admin/guidelines/Electronic%20Access%20Code%20Control%20Log.docx).
6. The senior-level employee should change the electronic access code whenever an employee leaves employment or is transferred to another location. This should also be done in the event that the senior-level employee has reason to believe the code has been compromised.