**Control of Access to Campus Facilities** **UPPS No. 08.02.01**

 **Issue No. 9**

 **Revised Date: 05/02/2022**

 **Effective Date: 06/09/2020**

 **Next Review Date: 10/01/2025 (E5Y)**

**Sr. Reviewer: Director, Facilities Operations**

**POLICY STATEMENT**

*Texas State University is committed to providing a safe and secure environment, as well as safeguarding its assets and resources.*

**01. SCOPE**

01.01 Texas State University’s access control policy is the framework by which all keys and facility access credentials are issued, duplicated, stored, controlled, returned, replaced, and accounted for to maintain security of facilities, equipment, furnishings, books, and confidential material.

**02. KEY AND ELECTRONIC ACCESS CONTROL SYSTEMS**

02.01 Ingress Management Services designs key systems for use in university facilities. Ingress Management Services must approve all key systems used or installed on university-controlled property or facilities.

02.02 Ingress Management Services is responsible for the management of the university keying systems. That responsibility includes controlling the production, storage, and issuance of keys; the replacement or re-keying of lock cylinders; the acquisition of new keying systems; and the maintenance of accurate records. All locks and keys must be approved by Ingress Management Services before installation, and only Ingress Management Services may operate secure key duplicators, core pinning equipment, and interchangeable core control keys.

02.03 Ingress Management Services is responsible for the management, installation, and maintenance of campus-wide electronic access control systems using the Texas State ID card (also known as the Bobcat Card) to allow access.

02.04 Access Levels and Required Authorizations

1. Level 1 Access – This access level provides access to a room or office within a building. Authorization is granted by the access administrator for the assigned space.
2. Level 2 Access – This access level provides access to a group of rooms within a department or building. The issuance of this access permission is restricted to persons authorized by the key holder’s departmental chair or director.
3. Level 3 Access – This access level provides building-level access to all or most spaces within an individual building. The issuance of this access permission is restricted to persons authorized by the key holder’s departmental chair, director, or dean, with final approval granted through the appropriate vice president, and the vice president for Finance and Support Services (VPFSS). Multi-departmental buildings will require approval from all associated departmental chairs, directors, or deans, with final approval granted through each associated vice president and the VPFSS.
4. Level 4 Access – This access level provides access to all buildings within a particular key system on campus using keys checked out of a key watcher cabinet. The issuance of this access permission is restricted to persons authorized by the departmental chair, director, or dean, with final approval granted through the appropriate vice president, the VPFSS, and the president; such an access permission is restricted to essential need only.
5. Level 5 Access – This access level provides access to all buildings within a particular key system on campus via keys assigned to the key holder. The issuance of this access permission is restricted to persons authorized by the departmental chair, director, or dean, with final approval granted through the appropriate vice president, the VPFSS, and the president; such an access permission is restricted to essential need only.
6. Off-Master Keys – These keys provide restricted access to a room or a building reviewed and authorized to be off the university master key system. Issuance of this key is restricted to persons authorized by the VPFSS and the president. Any request for keying a space off the university master key system requires authorization by the president. Off-master areas will be reviewed every five years by Ingress Management Services to establish if the restricted off-master key is still warranted. If such security is no longer warranted, the secured environment will be placed back on the university master key system.

**03. INGRESS MANAGEMENT SERVICES KEY FILES**

03.01 Ingress Management Services will maintain a complete set of keys of all university facilities, buildings, and locks in a secure monitored location with a multi-method access log showing each instance the keys are accessed and by whom.

**04. MANUFACTURE OR DUPLICATION OF KEYS**

04.01 The manufacturing, cutting, or duplicating of any secure key for university property by a person other than the university locksmith is forbidden, and offenders will be subject to disciplinary action.

**05. KEY ISSUANCE AUTHORITY**

05.01 Ingress Management Services will issue and document the issuance of all keys to university facilities.

05.02 Access administrators are persons who are authorized to request the issuance of keys or electronic access to buildings or rooms under the control of their department or division. The access administrators for each department or division are appointed in writing by their departmental chair, director, dean, associate vice president, or vice president. The access administrator will perform staffing necessary to obtain approvals for access requests, as outlined in Section 02. Access administrators must be full-time university employees. Ingress Management Services will maintain a list of authorized access administrators.

05.03 Access administrators will be responsible for maintaining records of keys and electronic access permissions issued by Ingress Management Services at their request. Access administrators will act as department liaisons between Ingress Management Services and their respective department or division. Ingress Management Services will coordinate with access administrators to audit key issuances and electronic access permissions of the key holders within their department or division.

**06. KEY AUDIT PROCEDURES**

* 1. Ingress Management Services will conduct annual audits of issued keys.
1. Ingress Management Services will maintain employee key records. Ingress Management Services will provide access administrators with reports of key records grouped by department as requested. Ingress Management Services will coordinate with access administrators to reconcile the department’s records and Ingress Management Services’ records.
2. Ingress Management Services may conduct physical on-site audits of individual or departmental keys at any time.
3. Ingress Management Services will coordinate with access administrators to assist them with annual physical inventories of all grand master keys and off master keys.

**07. PROCEDURES FOR OBTAINING AND RETURNING KEYS**

07.01 Issuance of Keys

1. All faculty, staff, and students of Texas State may be issued keys for access to their workspace. In most situations, keys will be issued directly to the key holder. As key holders, individuals assume responsibility for the safekeeping, responsible use, and eventual return of university keys to Ingress Management Services.
2. All key requests must be made by the access administrator using the [AssetWorks AIM work order management system](https://aim.facilities.txstate.edu/fmax/login) maintained by Facilities. All key and electronic access requests must be made by the appropriate access administrator. Ingress Management Services will approve all key and electronic access requests based upon policy and access requirements. All key requests must include the key holder’s full name, net ID, Texas State identification number, and the room or specific door the key holder needs to access.
3. Ingress Management Services will charge to recover the costs of cutting requested keys.
4. Replacement key requests for keys lost, unreturned, or stolen require a University Police Department (UPD) incident case number be included in the request. Replacement key requests require the person’s supervisor or director approvals (see Section 11.). Keys issued to students for residence hall rooms are exempt from this requirement.
5. The key holder being assigned a key must pick up the key in person. Only under extreme circumstances will there be exceptions to this rule.
6. Keys requested for key holders at the San Marcos campus will be issued at Ingress Management Services. Keys requested for key holders at the Round Rock Campus will be issued at the Facilities Operations office at the Round Rock Campus.
7. All requested keys must be picked up within 30 days or the request is void, and a new request will need to be completed before a key can be issued. Keys requested, but not picked up, may result in the division or department being charged if a key was cut for the request.
8. Ingress Management Services will provide each key holder with an electronic copy of their key issuance form for their personal record. It is the responsibility of the key holder to provide a copy to their access administrator.
9. The keys issued to a key holder are intended for use by that person only.

07.02 Returning of Keys

1. The key holder must return all keys to Ingress Management Services. Keys issued at the San Marcos campus will be returned to Ingress Management Services. Keys issued at the Round Rock Campus will be returned to the Facilities Operations office at the Round Rock Campus.
2. University keys must be returned when key holders separate from university employment, retire, resign, transfer to another department, move to a new office or workspace, or the keys are otherwise no longer needed. Ingress Management Services will provide the keyholder an electronic copy of the completed issuance form indicating the key has been returned upon key return. It is the responsibility of the key holder to provide a copy to their access administrator.
3. Keys must not be transferred from the key holder to another person. Keys must be returned and verified by Ingress Management Services before being issued to a new key holder. Departments may not retain keys in anticipation of an employee replacement, transfer, or termination.

07.03 Keys to Housing and Residential Life Facilities

1. The associate director, Housing Facilities Services in the Department of Housing and Residential Life (DHRL) is responsible for the management of building access and key control procedures for residence halls, residence room, or apartment keys for use by residents and departmental employees.
2. DHRL will maintain procedures and records for key control in line with this policy and approved by Ingress Management Services.
3. An access administrator will be designated by the director of DHRL.
4. Keys issued to DHRL as replacement keys for residence halls will be delivered to the front desk of each housing facility or to the DHRL access administrator.
5. DHRL is authorized to charge the resident for costs associated with lost keys and the expense of re-keying to recover both actual costs (labor, materials, and markup) and administrative costs required to process the work request. DHRL will initiate these charges.

07.04 Departmental Keys

1. Departments may maintain departmental keys, access level 3 or below, for short-term use by employees to perform tasks, but who do not need a permanently issued key. The access administrator will perform staffing necessary to obtain required approvals for these keys, as outlined in Section 02. Departments are responsible for the security of these keys. Departmental keys should be stored in a secure area (lockable box or cabinet), and a check-out system approved by Ingress Management Services should be established to track who has the key. At a minimum, the check-out procedures should document when the key was checked out, when it was returned, and the individual responsible for the key. These keys must be issued to and managed by a person delegated by the department to be responsible for their use and safekeeping. Departmental key storage and check-out procedures are subject to audit by Ingress Management Services.

**08. PROCEDURES FOR SECURITY OF MASTER KEYS (ACCESS LEVEL 3 – 5)**

08.01 This section outlines the procedures to limit the risk to the university posed by master and grand master keys.

1. Ingress Management Services will issue master keys to the minimum number of employees necessary to perform needed functions.
2. Master keys must not leave university property.
3. Ingress Management Services will issue master keys directly to the specified individual, with the exception of the DHRL facilities; such responsibility is delegated to the associate director, Housing Facilities Services in the DHRL, or designee.
4. Those individuals issued master keys should physically secure the keys when not in personal use in an electronic key box, key safe, or unmarked, locked cabinet or drawer inside a locked area.
5. Ingress Management Services may conduct audits of key control practices.

**09. ELECTRONIC ACCESS SECURE KEYWAY PROCEDURES**

09.01 Ingress Management Services may key all doorways equipped or controlled with electronic access control to a separate keyway maintained for electronic access. Ingress Management Services will determine whether an area implementation of the secure keyway is appropriate or warranted.

1. Only UPD, the associate director, Housing Facilities Services, and locksmiths will be issued master keys that operate the secure keyway.
2. Issuance of change keys to individual doors or groups of doors equipped with this keyway shall be limited to one or two keys only.
3. Keys issued to this keyway will be subject to an on-site physical key audit at least once every two years.
4. Master keys issued to this keyway require annual physical on-site audits.
5. Re-keying is mandatory if a secure keyway key is lost or misplaced.

**10. PROCEDURES FOR SEPARATELY AND OFF-MASTER KEYED OFFICES**

10.01 University master, GM, GGM, GGGM keys cannot open separately keyed or off-master keyed offices.

10.02 UPD and Ingress Management Services will provide a security and keyway analysis for all requests when receiving a request for a separately keyed area.

10.03 The president must approve requests to key an office or other area separately from the university grand master system.

10.04 Ingress Management Services will conduct annual audits of keys issued for separately keyed or off-master areas.

**11. PROCEDURES REGARDING LOST, STOLEN, OR UNRETURNED KEYS**

11.01 Individuals and departments must immediately report all lost, stolen, or unreturned keys to Ingress Management Services and file a police report with UPD.

11.02 UPD, in cooperation with Ingress Management Services and other appropriate departments and divisions, shall develop and provide a written report to the VPFSS outlining the exposure and risk posed by the lost, stolen, or unreturned key, strategies for mitigating the loss, and estimated costs to re-key the associated locksets and replace all current key holders’ keys. Keys issued to students for residence hall rooms are exempt from this requirement.

11.03 Departments whose employees lose a key or fail to return an issued key will pay to re-key all doors or buildings affected by replacing all current key holders’ keys in addition to the cost to re-core the locksets. The VPFSS and the director of Facilities Operations will decide the scope of any mitigation plan.

**12. PROCEDURE FOR KEYS ISSUED FOR CONSTRUCTION OR CONTRACT SERVICES**

12.01 Ingress Management Services will not issue keys directly to a contractor. When university keys are required to be issued to contractors or contracted service providers working on campus, keys needed will be determined by Ingress Management Services for the project manager or the department managing the contracted service. The keys will be issued to the department managing the contracted service. The key information will be recorded on a Contractor Key Agreement form to be signed by the contractor representative or contracted service provider. Departments managing contractors or contracted services should ensure contracts detail the contractor’s responsibility for reestablishing security of the areas affected if the keys are not returned.

**13. ELECTRONIC ACCESS CONTROL PROCEDURES**

13.01 Electronic access-controlled doors are for the areas accessed by individuals by way of a Texas State ID card, temporary access card, I-button fob, or pin code. Access to individual doorways or groups of doors are controlled by adding or removing individuals from electronic access permission groups. The permission groups are administered by Ingress Management Services at the request of access administrators who oversee the spaces controlled based upon access level authorization requirements outlined in Section 02.

13.02 Normally, keys are not issued to any electronic access control doors to include locks that use a Texas State ID card, temporary access card, I-button fob, or pin code to gain access. Keys will only be issued to electronically controlled doors on the electronic access secure keyway for designated police officers and locksmiths. All requests for exceptions based on business need to this rule must be submitted in writing to the VPFSS, or designee. If an exception is allowed, the door lock will be changed to an individual room key with a limited number of keys issued based on the same business need. The door lock will also be placed under the normal university master key system and removed from the electronic access secure keyway.

13.03 Students, faculty, and staff are required to maintain a Texas State ID card for access. Contractors, vendors, and volunteers must apply for access through the sponsoring department's access administrator.

13.04 The access administrator will request electronic access permissions for individuals to be added or removed by using the [Asset-Works AIM](https://aim.facilities.txstate.edu/fmax/login) work order management system maintained by Facilities.

13.05 Individuals not able to obtain a Texas State ID card will be issued a temporary access card by Ingress Management Services at the request of the sponsoring department's access administrator. Temporary access cards will be issued with expiration dates, so that the sponsoring department's access administrator may audit and control access. Upon request, Ingress Management Services will provide the access administrator with a list of temporary access cards issued. Ingress Management Services will coordinate with the access administrator to audit temporary access cards annually.

\*13.06 Ingress Management Services will not issue temporary access cards directly to the contractor for construction or contracted services. Electronic access permissions needed will be determined by Ingress Management Services, in consultation with the project manager or department managing the contracted service. Temporary access cards will be issued to the access administrator of the department managing the contracted service.

13.07 Tampering with or attempting to bypass security on an electronically- controlled or monitored door in any way, including, but not limited to, key bypass, propping, taping, and dogging is prohibited.

13.08 The departmental access administrator will have the overall responsibility of ensuring that the building users are using the electronic access control system and not bypassing it. Reported and uncorrected violations of this and other security incidents resulting in unauthorized entries to buildings or false alarms will be investigated and corrective actions taken, including, but not limited to, termination of access.

13.09 Upon request, Ingress Management Service will provide the access administrator with a list of individuals assigned to the department’s or division’s electronic access permission groups. Ingress Management Services will coordinate with the access administrator to audit electronic access permission groups annually.

**14. REVIEWERS OF THIS UPPS**

\*14.01 Reviewers of this UPPS include the following:

Position Date

Director, Facilities Operations October 1 E5Y

Director, University Police Department October 1 E5Y

Executive Director, Housing and October 1 E5Y

Residential Life-Housing Facilities

Services

Associate Vice President for Facilities October 1 E5Y

Vice President for Finance and October 1 E5Y

Support Services

**15. CERTIFICATION STATEMENT**

This UPPS has been approved by the following individuals in their official capacities and represents Texas State policy and procedure from the date of this document until superseded.

Director, Facilities Operations; senior reviewer of this UPPS

Associate Vice President for Facilities

Vice President for Finance and Support Services

President