2.401 ACCESS CONTROL *(17.5.2)*

2.401.02 General Provisions

A. Employees who are issued keys or granted electronic access for use in their duty assignments will:
   1. Access areas only in the performance of *bona fide* job tasks;
   2. Account for, and provide appropriate levels of custody and security to, their issued keys and access cards;
   3. Promptly report and document damaged, broken, lost, or stolen keys or access cards to a supervisor or commander as appropriate;
   4. Return keys to the key coordinator or location from where the keys were obtained as directed;
   5. Request new, replacement, or additional keys or electronic access only by using the key request process;
   6. Return all long-term issued keys when they leave the agency or their duty assignments change such that they no longer need the keys; and
   7. Follow applicable key and access control directives.

B. Employees will not:
   1. Loan keys except in extreme emergencies;
   2. Duplicate keys; or
   3. Alter keys or any accompanying key rings.

C. Employees will use their electronic access cards instead of traditional keys to access electronically controlled areas on-campus unless exigent circumstances exist.

D. Loss, damage, etc. to keys, key rings, electronic access cards, etc.:
   1. That is discovered after keys have been issued will be construed to have occurred while in the possession of the assigned user; and
   2. Will be reported and administratively reviewed consistent with **1.432 Resource Care and Maintenance**.

E. See also **TU 07-17.00 Key Control & Card Access Policy**; and

F. See also **2.401.12 Separated Employees and Post-Separation Access**.

2.401.04 Key Coordinator

A. The Logistics Officer is designated as the agency's key coordinator. The administrative assistant to the Logistics Officer's commander serves as the agency's alternate key coordinator.

B. The key coordinator has duties and responsibilities that include, but are not limited to:
   1. Those specified in **TU 07-17.00**;
   2. Securely maintaining the agency's supply of surplus and back-up keys;
   3. Receiving all long-term issued keys as they are turned in by employees when they leave the agency or their duty assignments change and they no longer need the keys;
   4. Ensuring employees sign for transactions involving long-term issued keys;
   5. Returning keys that have no reasonably foreseeable uses to the central key coordinator;
   6. Inform TU Access Control when employees separate or otherwise no longer require electronic access, consistent with **2.401.12**; and
   7. Conducting key inventories and access control audits as directed.

2.401.06 Access Requests

A. Employees will request keys or electronic access consistent with **1.433 Service Request System** and **UPO.114.D Procurement Request** through their respective chains of command for:
   1. New, replacement, or additional keys; or
   2. Maintenance on locks within the agency.

B. Key and access requests that have been approved by a commander must be coordinated through the key coordinator's commander for final approval and submission to the central key coordinator.

2.401.08 Issued Keys

A. Some keys may be issued to employees for long-term duty needs, such as office keys, desk and file cabinet keys, and will be returned to the key coordinator when employees:
   1. No longer need the issued keys;
   2. End their employment with the agency, consistent with 2.401.12;
   3. Are granted a leave of absence for 30 or more days; or
   4. Are ordered to do so by a superior.

B. Some keys may be temporarily issued to employees for short-term duty needs, such as vehicle keys, master key rings, etc. Employees will turn these keys back in when they:
   1. End their tours of duty or duty assignments that necessitated the keys being issued; or
   2. Are ordered to do so by a superior.

C. The electronic key box is the primary repository for keys that are issued on a temporary basis.
   1. Employees will:
      a. Access the key box only to check keys in and out as authorized;
      b. Check keys in and out properly and on a timely basis to facilitate accurate electronic key tracking; and
      c. Promptly notify supervisors and complete **Loss / Damage Reports (UPO.079.D)** consistent with **1.432.08 Administrative Reporting** when keys are missing or damaged.
   2. Patrol supervisors will ensure:
      a. All keys are accounted for each shift; and
      b. Compliance with **1.432 Resource Care and Maintenance** when keys are missing or damaged.

2.401.10 Key Control Audits & Inspections

A. A 100% departmental key audit will be conducted and documented whenever a new key coordinator is designated. These audits will be conducted by the new key coordinator and at least one other employee designated by the Chief. The key coordinator's commander or designee will investigate and attempt to resolve all audit discrepancies before the new key coordinator assumes full duty accountability.

B. Regular key audits will be conducted consistent with **TU 06-17.00**.

C. The inspections commander may have unannounced, random inspections conducted on:
   1. The key coordinator's records and related items; and
   2. Other records relating to key control.

D. Inspection reports will be reviewed, commented on, and approved by the inspections commander before being submitted to the Chief and others as appropriate. The inspections coordinator will retain finalized inspection reports for at least three years.

2.401.12 Separated Employees and Post-Separation Access

A. For purposes of this directive, separation includes resignation, retirement, non-renewal of employment, involuntary termination, separation in lieu of termination, or any other end of employment with the Towson University Police Department.

B. Upon the effective date and time of an employee's separation from the agency, the employee's physical and electronic access to non-public and secure areas of TUPD facilities will be terminated.

C. The key coordinator, or designee, will coordinate with TU Access Control in advance whenever practicable to ensure the separated employee's electronic access privileges are deactivated effective as of the employee's separation date and time, unless otherwise directed by the Chief of Police or designee.

D. Prior to leaving the agency, separating employees will return all issued keys, access cards, identification credentials, badges, and any other issued agency property to the Key Coordinator, Support Services Bureau Commander, or other designated agency representative whenever practical. Separating employees will also remove all personal property from lockers, offices, and other assigned work

areas before their final tour of duty. If a separated employee needs to retrieve personal property after separation, the employee must coordinate the visit in advance through the Office of the Chief, bureau commander, or designee, and must remain under escort at all times while in any secure or non-public area.

E. Separated employees will not be permitted unescorted access to secure or non-public areas of TUPD facilities. Secure areas include, but are not limited to, the Communications Center, Records area, Property/Evidence areas, Patrol areas, Criminal Investigations areas, command offices, and other areas not open to the general public.

F. Separated employees may access public areas of TUPD facilities in the same manner as other members of the public. Access beyond public areas requires approval from supervisory ranked personnel and an official escort.

G. Active employees will not allow a separated employee to enter secure or non-public areas by using another employee's access card, keys, credentials, or by permitting the separated employee to follow them through a controlled access point unescorted.

H. When an active employee is the subject of an internal investigation or presents an identified safety, security, CJIS, evidence, or operational concern, the employee's access to secure or non-public areas may be restricted or suspended as authorized by the Chief of Police or designee.

I. A separated employee whose employment ended through involuntary termination or separation in lieu of termination, or who presents an identified safety, security, CJIS, evidence, or operational concern, shall be prohibited from accessing secure or non-public areas, including access that would otherwise be permitted with an escort, unless specifically authorized by the Chief of Police or designee.

J. If an identified safety or security concern exists regarding a separated employee, an internal agency safety or security notification may be distributed as authorized by the Chief of Police or designee.