Access Control Services
Access Levels and Authorization Requirements

Each Access Level has required authorization that demands signed approval from University Authorizers on an Alarm Code Authorization Form. Some Access Levels may require more than one Director, Chair, Dean, or AVP to sign their approval since a University Authorizer may only sign to approve the issuance of a Security Alarm Code for locations over which they have full authority. Every Security Alarm Code approval also requires the signature of the Code Holder and their direct Supervisor. The following table displays the Access Levels, their required authorization, and examples of each:

Access Levels	Authorization Required	Examples
1 – Campus Wide	President, Supervisor & Code Holder	UPD officers needing access to all locations on campus to properly perform their duties
2 – Multiple Buildings	Dean/AVP, Supervisor & Code Holder	Maintenance, ITS, or custodial employees needing access to every part of more than one building to perform their duties
3 – Full Building	Dean/AVP, Supervisor & Code Holder	Custodians or departmental associates needing access to every part of a single building within their scope of duty, responsibility, or authority
4 – Multiple Partitions	Director/Chair, Supervisor & Code Holder	Faculty or staff needing access to multiple parts of a single building within their scope of duty, responsibility, or authority
5 – Single Partition	Director/Chair, Supervisor & Code Holder	Faculty or staff needing access to a single part of a single building within their scope of duty, responsibility, or authority

Roles and Responsibilities

AVPs and Deans are responsible to authorize the issuance of any Security Alarm Code requiring access to a full building (Level 3) or multiple full buildings (Level 2) for the University facilities allocated to their department.

Code Holder is responsible for maintaining the confidentiality of their personal Security Alarm Code and informing the Security Alarm Manager and their Supervisor if that confidentiality is compromised. Code Holder is further responsible for obtaining the key and/or card swipe access from Access Control for the location(s) to which they have Security Alarm Code access.

Department Chairs and Directors are responsible for authorizing the issuance of any Security Alarm Code requiring access to a single partition (Level 5) or multiple partitions in a single building (Level 4) for the University facilities allocated to their department.

Security Alarm Manager is responsible for determining the level of access required by the requested Security Alarm Code, establishing whom the appropriate University Authorizer(s) and Supervisor(s) are, creating an Alarm Code Authorization Form for each request, obtaining signatures from all involved parties in the Security Alarm Code Authorization process, and retaining the signed form through the appropriate software. The Security Alarm Manager is further responsible for assigning, activating, and privately issuing the Security Alarm Code to the Code Holder and training new Code Holders on how to arm and disarm the security alarm and clear faults.

Supervisors are responsible for authorizing the issuance of any Security Alarm Code of any access level required by any of their direct subordinates. Supervisors are further responsible for requesting key and/or card swipe access from Access Control for their direct subordinates who they have authorized to have a Security Alarm Code. Note that supervisors may also be University Authorizers. A University Authorizer—with full authority over the access level required—who authorizes the issuance of a Security Alarm Code for a direct subordinate eliminates the need for another Supervisor's authorization.

The President or their designee is responsible for authorizing the issuance of any Security Alarm Code requiring access to all University facilities campus-wide (Level 1).