
	<b>GAITHERSBURG POLICE DEPARTMENT</b>			
	<b>KeyWatcher System Use</b>			
	<b>GENERAL ORDER</b>	<b>108.16</b>		Related CALEA Standards:
	<b>Effective Date</b>	<b>04/24/2024</b>		
<b>Authorized by:</b>	<b>Mark P. Sroka</b> CHIEF OF POLICE	SIGNATURE	DATE 04/24/2024	

## 1. PURPOSE

- 1.1 The purpose of this directive is to designate the central control point for all GPD keys and locks used for vehicles, equipment, or used to secure the doors of space owned, occupied, leased or loaned to Gaithersburg Police Department. Gaithersburg Police Department utilizes the KeyWatcher electronic storage and tracking system to grant access to vehicle and master keys.

## 2. POLICY

- 2.1 It is the policy of this department that keys and locks used to secure vehicles, equipment or the doors of space owned, occupied, leased or loaned to Gaithersburg Police Department provide for the safety of employees and visitors.

## 3. DEFINITIONS

- 3.1 **Access** – Method of entry to a physical space, vehicle or lock that is restricted to certain individuals either on a permanent basis or during certain hours of the day.
- 3.2 **Access Credential** - Key, key card, phone app, fob, access code, or any authorized device that gives access to a space.
- 3.3 **Audit Trail** - Documentation establishing access credentials assigned to individuals used at a particular time and place.
- 3.4 **Building Master** - Access credentials that work all the door locks in a building.
- 3.5 **Credential owner** – An individual that has been issued a GPD key card credential.
- 3.6 **Key** - A single access key that works a single lock.
- 3.7 **Unit Master** - access credential that works all locks in a particular unit.
- 3.8 **Employee** – A person employed by GPD who is issued an identification number.
- 3.9 **Floor Master** - A sub master that works all door locks on a building floor.
- 3.10 **Great Grand Master** - Access credential that accesses all locks of similar type (e.g. electronic, hard key, etc.) except secured spaces.
- 3.11 **Human Resources** - Department within the City of Gaithersburg responsible for hiring and terminating personnel.
- 3.12 **KeyWatcher Administrator** – A person designated by the Chief or Administrative Bureau Commander with authority for the approval of access to the KeyWatcher Management System.
- 3.13 **Key Card** – A credential that allows access to spaces via electronic locks.
- 3.14 **Key Fob** – A credential that allows access to spaces via proximity or at a button press.
- 3.15 **Key Holder** – An individual issued any form of credential.
- 3.16 **KeyWatcher** - KeyWatcher is a brand name for an electronic key tracking box. Users can be granted access to remove keys that they are approved for. Access is

through a User ID and a Pin, there are different levels of access and time periods for having the keys checked out. Keys can be restricted to one or a few users or to many. There are many alarms and warnings that let the department know when keys are not returned, if the box is left open, or if the key is inserted incorrectly.

- 3.17 **Lock Box** – A controlled storage box, permanently affixed in some manner as approved by GPD for the storage of credentials to be shared by multiple users within a department. A KeyWatcher is a type of lock box.
- 3.18 **Master** - Access credentials that work multiple doors or multiple locks.
- 3.19 **Metal Key** – A credential which is a physical metal key.
- 3.20 **Non-Employee** – Any individual not possessing a City of Gaithersburg ID number. Examples include, but are not limited to vendors, contractors, and visitors.
- 3.21 **Secured Space** - A GPD physical space for which all access needs to be explicitly authorized, and therefore cannot be accessed with a master key.
- 3.22 **Security Services Grand Master (SSGM)** - Key card that accesses all electronics locks within GPD.
- 3.23 **Sub Master** - Access credential that works several doors but not all doors in a building.
- 3.24 **Volunteer** – An individual registered as an official volunteer for GPD. If these individual needs access to GPD buildings, then an identification number will be issued. This individual is expected to comply with all relevant aspects of this policy.

#### 4. **RESPONSIBILITIES**

- 4.1 Employees issued keys or given access to keys are responsible for ensuring that keys are not loaned or shared and will surrender all keys when transferred or separated.
- 4.2 All access requests will be approved by the appropriate supervisor or KeyWatcher administrator. If that supervisor is not available within a reasonable timeframe, the next higher supervisor in the Department may authorize requests.
- 4.3 Keys must be returned to the KeyWatcher no later than the end of shift by the same authorized individual who checked them out. Any person who has an overdue access credential that has not been returned will not be issued any further credentials until the overdue credential is returned or an extension request is submitted.
- 4.4 Employees and/or volunteers shall not "exchange" keys, fobs, or other access credentials when ending their shifts. Keys, fobs, or other access credentials must be returned to the KeyWatcher box and checked out by the next employee/volunteer who needs the item.
- 4.4 Lost or stolen keys need to be reported immediately to a supervisor within GPD who will notify the Keywatcher administrator.
- 4.5 Employees are responsible for reporting lost, stolen or damaged keys.
- 4.6 Use of keys are restricted for access to spaces or vehicles based on a legitimate business need.

#### 5. **KEY CONTROL**

- 5.1. Employees will be granted keys upon request and is based on an evaluation of the potential **key holder's** business purpose for access to a particular space, equipment or vehicle.
- 5.2. Personnel who are authorized by the Chief of Police, Bureau Commanders or Keywatcher Administrator may be granted access to keys.
- 5.3. All other keys will be issued by the KeyWatcher Administrator upon request of the appropriate Bureau Commander or Chief of Police.
- 5.4. Vehicle keys and building keys, fobs, keycards are kept in the KeyWatcher box.
- 5.5. Re-keying any lost/stolen key (other than file cabinets, desks, etc.) will require equipment operated by the lost keys, to be rekeyed and the costs to be covered by the employee that had was in the possession of the keys.
- 5.6. Lost/stolen key(s) will be replaced after the doors operated by the lost/stolen keys, have been rekeyed.

## 6. **FOB OR KEYCARD CONTROL**

- 6.1. ID cards are the sole property of GPD and must be returned upon request, termination or the end of active employment status.
- 6.2. GPD and Human Resources are authorized to issue, replace and revoke GPD ID badges.
- 6.3. Vendors and contractors are required to have a badge while on GPD property.
- 6.4. While at GPD badges must be visible and above the waist, unless work prohibits for safety reasons.
- 6.5. Persons with access to the KeyWatcher System will have the ability to request key, fob, or keycard access. Requests will be sent to the designated KeyWatcher Administrator, Chief of Police, or Bureau Commander who review and approve or deny the request.

## 7. **AUDITS**

- 7.1 Audit Trails of electronic key access records will only be made available by a request from Human Resources, the Chief of Police, Internal Affairs Commander or appropriate Bureau Commander. Additional requests for audit trail information may be made and handled on a case-by-case basis.
- 7.2 Audits on the KeyWatcher system should be conducted periodically.

## 8. **RESPONSIBILITIES OF ACCESS CREDENTIALS (KEY, FOB OR KEYCARDS)**

- 8.1. Access credentials are the responsibility of the individual to whom they are issued and shall not be shared with any other person. Loaning and lending of any access credential to another person is prohibited.

- 8.2. In instances where individuals need access to a space to which they do not have access credentials, they should submit a request in advance to the Keywatcher Administrator for that individual to have access granted to obtain an access credential from the KeyWatcher. If employees require access to a space to which they do not have access credentials and have a legitimate business purpose to enter that space, the Keywatcher Administrator controlling the space may grant that access.
- 8.3. If the need is present outside of business hours, the Keywatcher Administrator or designee can be called to request the space be opened on as-needed basis if exigent circumstances exist.