POLICY

It is the policy of the District to implement security safeguards to protect assets, records, information, confidentiality, and privacy.

These security safeguards must be applied in all administrative, physical, and technical areas and should use locks, guards, administrative controls, and other protective measures such as video surveillance to protect against loss or damage from intentional acts, accidents, fires, and environmental hazards such as water or wind.

SCOPE

Although physical security is a critical part of information security, there shall be a separate, more comprehensive policy for information security.

DEFINITIONS

Zones

A series of clearly discernible zones shall be used to progressively control access by the public and, to a lesser extent, by District personnel. The zones include:

Public Zone

The unrestricted area surrounding a facility or a designated part of a facility.

Examples include the parking lot, grounds surrounding a building, and public meeting rooms.

Boundary designators such as signs and direct or video surveillance may also be used to discourage unauthorized activity.

Reception Zone

Area where initial public contact occurs, where information is provided or exchanged, and access to restricted zones is controlled.

To varying degrees, activity in a Reception Zone is monitored by the personnel who work there, by other personnel, or by video surveillance.

Access by the public shall be limited to official business hours or for specific reasons.

Operations Zone

An area where access is limited to employees and properly escorted visitors, e.g., bays, day room, dorm room.

Operations Zones should be monitored at all times for proper identification and security breaches.

All guest and visitor's packages and materials taken into an Operations Zone must be inspected.

Visitors may be given special permission to be in the Operations Zone without an escort; e.g., public meeting, large groups of people on tour, training classes, vendor making repairs, etc.

Security Zone—An area to which access is limited to authorized personnel and to authorized and properly-escorted visitors, e.g., offices, storage rooms/closets, attics, etc.

Security Zones should preferably be accessible from an Operations Zone, and through an entry point, e.g., a door.

Entrance to Security Zones shall be monitored by the personnel who work there, by other personnel, and preferably by video surveillance.

Official Business Hours–The days and hours the facility is open for administrative purposes as determined by a Standing Rule of the Board of Directors.

RESPONSIBILITY

It is the responsibility of all **employees** to comply with this policy and exercise prudent judgment regarding the security of individual office and general work areas. Additionally, where applicable, employees are jointly responsible for security of the entire facility, vehicles, equipment, and supplies. Specifically, employees must:

- Understand their security responsibilities and duties;
- Understand the consequences of failure to adhere to this policy
- Immediately notify the Facility Manager if their identification badge and/or facility access is compromised, e.g., lost keys; and
- Immediately notify the Facility Manager, Fire Chief, or District Manager if there is noncompliance to this policy.

It is the responsibility of the **District Manager** and **Fire Chief** to:

- Monitor the adherence to the policy;
- Educate their respective employees on the requirements and their responsibilities in this policy;
- Ensure employee identification and keys are returned when no longer needed;
- Immediately notify the Facility Manager if their employee identification and/or facility access is compromised, e.g., lost keys; and
- Promptly notify the Information Security Officer of any noncompliance to the information technology portion of this policy.

It is the responsibility of the **Facility Manager** to:

- Monitor adherence to this policy;
- Implement a process for facility access accountability and control that is based on facility access granted on an as needed basis;
- Have facility access changed if access has compromised, e.g., lost keys;
- Ensure a facility uninterrupted power source (UPS) is available to all critical computer and voice systems and that the facility UPS is tested monthly;
- Ensure emergency (panic) hardware on "emergency exit only" doors is installed and emergency exits are properly marked;
- Ensure emergency lighting is available and tested monthly; and
- Ensure smoke and fire detection systems with alarms are installed and tested monthly.
- Ensure fire extinguishers are installed, checked monthly, and inspected annually.

PRACTICES

1. Access to the facility shall be progressively restricted and access controlled by the use of designated zones.

2. **Employees** shall not allow the public to use of District facilities and property by one or more members of the public without prior approval of the Facility Manager, including scheduling tours, public meetings, etc.

3. All **employees** shall ensure that when leaving facilities, that all doors, window, and window/door blinds are closed and locked.

4. The **Facility Manager** shall ensure that doors or access to such areas as storage rooms/closets and attics remain locked.

5. All **employees** should be alert for people who act in a suspicious manner, as well as objects, items, or parcels which look out of place or suspicious.

6. The **Facility Manager** shall keep trash and recycle bins areas away from buildings.

7. The **Facility Manager** shall post signs stating that firearms, illegal drugs, knives, and weapons of any kind are prohibited in District facilities except as allowed by law, e.g., RSMo 571.30(8).

8. The **Facility Manger** must approve electronic recording devices, cameras, and video cameras in operational and security areas.

9. **Employees** must escort guests in Operational and Security Zones.

10. The **Facility Manager** shall post signs stating that all visitors (vendors, guests, delivery personnel, etc.) are required to remain in Public and Reception Zones unless escorted or authorized to be unescorted.

11. All **employees** are required to prominently wear employee identification.

12. Without endangering themselves, **employees** should question unescorted visitors and report unauthorized or unescorted visitors. Identification badges should be removed or concealed when leaving the facility.

13. Only the **Facility Manger** may authorize visitors access to Security Zone. Access to certain Security Zones may require education on the District's confidentiality and privacy policies and practices.

14. **Employees** must protect assets by locking file and desk drawers and storing equipment, tools, and supplies in locked cabinets, shelves, and closets.

15. The **Facility Manager**, **District Manager**, or **Fire Chief** may issue special permission for visitors to be in facilities without an escort e.g., large groups of people on tour, training classes, vendor making repairs, etc.

16. Only the **Facility Manager**, **District Manager**, or **Fire Chief** may contact law enforcement when assets are found missing or intentionally damaged or broken.

17. The **Facility Manager** should ensure sufficient illumination in and around facilities to allow the detection and observation of persons approaching facilities and to discourage criminal activity.

18. Facilities and grounds should be built, organized, and maintained to minimize potential hiding places for trespassers and suspicious objects, items, or parcels.

19. The **Facility Manager** should ensure signs are posted indicating security measures are in place.

20. The **Facility Manager** shall implement a process for access accountability and control and the Facility Manager will maintain an Authorized Access List that names the personnel authorized to enter restricted areas with access granted on an as needed basis. If access is compromised, e.g., a key is missing, access must be changed.

21. **Employees** shall never lend District-issued keys to anyone.

<u>RELATED POLICIES</u>

Standard Operating Procedures or Guidelines 112
Employee Orientation 212
Personnel Files 254
Email and Internet Usage 588
Confidentiality and Privacy Policy 730
Information Security 858

<u>STATUTORY REFERENCE</u>

§571.30(8)

<u>REVISION HISTORY</u>

Revision Date	Author	Revision Details
March 12, 2022	Monte Olsen	Initial version