



Colorado Department
of Public Health
and Environment

Facilities Security Plan

This plan supplements the mandated procedures in department policy 15.19, “Secure Facilities.”

Physical Security

Building perimeters, office perimeters and perimeters for sensitive or restricted areas shall be of physically sound construction, with strongly constructed continuous floor-to-ceiling walls and appropriately sound and secured entryways. Delivery and loading areas shall be segregated from other department operations, particularly from sensitive and restricted areas, in order to control deliveries and to minimize access to the operating facilities.

In areas under video monitoring, notices shall be posted at entry points and at reception/guard areas indicating that video monitoring and other surveillance tools may record visitor actions.

Physical Access

Access to non-public areas shall be limited to authorized personnel. The mechanisms and procedures for restricting access to non-public areas shall be commensurate with the level of risk associated with each area.

Business Hours Access

The Cherry Creek campus security desk is staffed during all hours when the doors are open, Monday through Friday, 8:00 a.m. to 5:00 p.m. Key cards allow for employee entry Monday through Friday, 5:00 a.m. to 7:00 p.m. Supervisors must approve all after-hours access.

Visitors

Visitors are required to sign in and be issued a guest sticker that is to be worn while on the campus. Employees are contacted by the security desk when visitors are to be escorted to secure areas.

Security Maintenance

All repairs and modifications to the physical components of a facility – such as hardware, walls, doors and locks – must be documented and formal “change-management” procedures must be followed, in accordance with the following guidelines:

- Physical configuration changes to information technology facilities must be planned, approved and logged.
- Documentation of the technical configuration of information technology facilities must be produced immediately as part of the change-management process.
- Copies of configuration documentation must be stored offsite.

- Recovery planning must be performed as part of every change to ensure ongoing continuity of services in the event of complications.

Emergency Access

During a disaster-recovery situation, necessary steps may be taken under the direction of the security officer to ensure that a facility's access requirements fully support the disaster-recovery effort. Such steps may include temporary lockdowns and increasing access to certain areas. Normal access procedures must resume prior to or immediately after the resumption of normal business operations.