Approved by Douglas H. Benevento, Executive Director, April 11, 2005

SUMMARY

Access to Colorado Department of Public Health and Environment facilities must be controlled and monitored if the information systems, work places and sensitive information are to remain secure. Every staff person and workforce member has a role to play in ensuring that the facilities are secure.

POLICY

The department security officer has established a Facilities Security Plan, which limits access to department buildings, data processing and other internal secured areas to those users with a justified need to access them. All workforce members will support the steps needed to ensure facility security.

PROCEDURE

1. All workforce members are required to read and support the department Facilities Security Plan.
2. All employees must prominently display their department identification (ID) badge or register as a visitor.
3. All visitors – such as former employees, employee family members, vendors, consultants, repair contractors, maintenance staff, law enforcement officers and delivery service personnel – must prominently display a department guest pass with the current date.
4. Visitor identification shall only be issued after the visitor has signed the log at the designated sign-in desk and has completed the requested information, including the employee contact.
5. Employees must not permit unknown or unauthorized individuals to pass through un-staffed points of entry at the same time an authorized person is entering ("piggybacking").
6. Employees are prohibited from allowing access to any department facility to any person they do not know or to anyone not wearing a department identification badge.
7. Persons who are in a department building and are not wearing an identification badge should be asked in a friendly manner if they need assistance. If the visitor is not properly identified, the employee should attempt to escort the individual to the lobby area located in Building A or to the front desk at Laboratory and Radiation Services. The employee also can call Building Operations at extension 2113 or contact any supervisor. In the case of an extreme urgency, call 9-911.
8. Prior to granting a person access to a department facility, staff members will verify the status of the person by checking for a department ID tag through a secure door.
9. Program managers shall promptly revoke physical access rights to terminated personnel. Further, program managers, at their own discretion, may revoke access prior to the termination date.
10. No controlled access doors will be propped open.

11. Any individual with a key access card must report lost or stolen access cards – immediately upon discovery – to their supervisor and to either Building Operations at the Cherry Creek campus or the security officer at the Laboratory Services Division building.
12. Program managers must ensure that electronic equipment through which sensitive information may be obtained is located behind locked doors with controlled access. Such equipment includes host information systems that contain sensitive information as well as laptops, stored monitors and telecommunications gear.
13. Staff and visitors should understand that the department may use video monitoring or other surveillance tools for security purposes.
14. Supervisors will approve after-hours access for staff before a key access card will be issued. Either Building Operations at the Cherry Creek campus or the security officer at the Laboratory Services Division building will maintain documentation on all after-hours access keys.
15. Staff who arrange for the employment of temporary workers should ensure that those workers understand that they may not enter the building before 8 a.m.
16. If someone requests access to an internal controlled doorway, another staff member must verify the validity of the request, escort the person who lacks an access key, and ensure that such a person remain accompanied by a staff member while inside the secured area.
17. Individuals with after-hours keys should never give the key to another person. The key, once "swiped," registers the ID of the staff member to which the key was issued. This electronic registration is as valid as the signature. Those issued after-hours keys should be informed that key-usage reports are sent to supervisors for review.
18. Program managers should ensure that sensitive information can be locked away from unauthorized access and that keys are not left in the locks while workforce members are away from their work areas.
19. Any employee not complying with this policy and these procedures may be subject to state personnel system disciplinary action. Other non-employee workforce members will be disciplined with appropriate action, up to and including termination.
20. Program managers are encouraged to review approved forms and reports relating to after-hours access, conduct spot checks of secured rooms under their control, and from time to time test for accessibility to those areas without proper documentation.

21.
TOOLS/GUIDANCE/STANDARDS

Facilities Security Plan

REFERENCE

Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule §164.310, Physical Safeguards, Facility Access Controls (a)(1); (2) Implementation specifications: (i) Contingency operations, (ii) Facility Security Plan, (iii) Access control and validation procedures, (iv) Maintenance records