



## Physical Access Guideline

### Purpose

Physical access controls define who is allowed physical access to facilities that house information systems, to the information systems within those facilities, and/or the display mechanisms associated with those information systems. Without physical access controls, the potential exists that information systems could be illegitimately physically accessed and the security of the information they house could be compromised.

### Scope

This Physical Access Control Guideline applies to all facilities of Cornwall-Lebanon School District within which information systems or information system components are housed. Specifically, it includes:

- Data centers or other facilities for which the primary purpose is the housing of IT infrastructure
- Data rooms or other facilities within shared purpose facilities for which one of the primary purposes is the housing of IT infrastructure
- Switch and wiring closets or other facilities for which the primary purpose is not the housing of IT infrastructure

### Guideline Statements

1. Access to facilities, information systems, and information system display mechanisms will be limited to authorized personnel only. Authorization will be demonstrated through the use of authorization credentials (badges, identity cards, keys, etc.) that have been issued by Cornwall-Lebanon School District.
2. Access to facilities will be controlled at defined access points through the use of locked doors and cabinet racks. Authorized personnel are required to authenticate themselves at these access points before physical access to facilities, information systems, or information system display mechanisms is allowed. The delivery and removal of information systems will also be controlled at these access points. No equipment will be allowed to enter or leave the facility without prior authorization and all deliveries and removals will be logged.
3. A list of authorized personnel will be established and maintained such that newly authorized personnel are immediately appended to the list and those personnel who have lost authorization are immediately removed from the list. This list shall be reviewed and, where necessary, updated on an at least yearly basis.
  - Access to facilities will be granted to personnel strictly based on a job-related need.
4. Facility access cards/keys must have no identifying information aside from a return mailing address.
5. Facility access cards/keys will not be loaned or shared with others.
6. Any lost or stolen facility access cards/keys will have access removed and must be immediately reported to the district technology coordinator.
7. In the event that visitors need access to the facilities that house information systems or to the information systems themselves, those visitors must have prior authorization, must be positively identified, and must have their authorization verified before physical access is granted. Once access has been granted, visitors must be escorted and their activities monitored at all times.



# Cornwall-Lebanon School District



8. An access log will be maintained that records personnel access to facilities. This log will include the following:
  - Date and time of entry
  - Name of accessing individual and authentication mechanism
  - Name and title of authorizing individual
  - Reason for access
  - Date and time of departure
  
9. A delivery and removal log will be maintained that records equipment that is delivered to or removed from facilities. This log will include the following:
  - Date and time of delivery/removal
  - Name and type of equipment to be delivered or removed
  - Name and employer of the individual performing the delivery/removal and the authentication mechanism used
  - Name and title of authorizing individual
  - Reason for delivery/removal

## **Procedure 1**

Authorize, identify, and authenticate individuals that require physical access:

- Identify the roles that require both regular as well as occasional physical access and identify the individuals that fill these roles.
- Provide standing authorization and a permanent authenticator to individuals that require regular access.
- Require individuals who need occasional access to submit a request that must be approved prior to access being attempted or allowed.
- Authenticate individuals with regular access requirements through the use of their assigned permanent authenticator.
- Authenticate individuals with occasional access requirements through the use of a personal identification mechanism that includes name, signature, and photograph.

## **Procedure 2**

Verify that work to be performed has been pre-approved or meets emergency response procedures:

- Verify against standard change control procedures.
- Verify against standard maintenance procedures.

## **Non-Compliance**

Violations of these guidelines will be treated like other allegations of wrongdoing at Cornwall-Lebanon School District. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable Cornwall-Lebanon School District policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements.