# **Definitions**

**Information systems**: Is any combination of information technology and individuals’ activities using that technology, to support operations management.

**Display mechanisms**: A monitor on which to view output from an information system.

# **Overview**

Physical access controls define who is allowed physical access to {COMPANY-NAME} 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 exits exists that information systems could be illegitimately, physically accessed and the security of the information they house could be compromised.

**Purpose**

This policy applies to all facilities of {COMPANY-NAME}, 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

## **Policy Detail**

Access to facilities, information systems, and information system display mechanisms will be limited to authorized personnel only. Authorization will be demonstrated with authorization credentials (badges, identity cards, etc.) that have been issued by {COMPANY-NAME}.

Access to facilities will be controlled at defined access points with the use of card readers and locked doors. Before physical access to facilities, information systems, or information system display mechanisms is allowed, authorized personnel are required to authenticate themselves at these access points. 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.

A list of authorized personnel will be established and maintained so 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 at least an annual basis.

If 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.