



Michelle Lujan Grisham
New Mexico Governor
Raja Sambandam
Acting Cabinet Secretary & State CIO

Policy Title:	Physical Access Control Policy
Policy Number:	DoIT-361-713
Effective Date:	June 14, 2022
Issued By:	DoIT CIO
Distribution:	DoIT IT Resource Users
Approved by:	Raja Sambandam, Acting Cabinet Secretary

1. AUTHORITY

Pursuant to the New Mexico Department of Information Technology Act, NMSA 1978, § 9-27-1 *et seq.*, the Secretary of the Department of Information Technology (DoIT or Department) shall exercise general authority over all Department employees, manage all operations of the Department, and administer and enforce the laws with which the Secretary or the Department is charged.

Pursuant to NMAC 1.12.20.12, to preserve the integrity, confidentiality, and availability of the system and data, DoIT's information assets must be protected by logical as well as physical access control mechanisms commensurate with the value and sensitivity of the system, the ease of recovery of the assets, and the direness of consequences, legal or otherwise, if loss or compromise were to occur.

2. PURPOSE

This Policy presents guidelines, roles, and responsibilities associated with ensuring the physical security of DoIT facilities, systems, and personnel.

3. SCOPE

This Policy applies to all DoIT facilities, systems, and DoIT IT Resource Users.

4. DEFINITIONS

- a. **Access Control System** - An automated system that manages personnel access to secure locations, and has the ability to lock, unlock, track, and record door access and to alert monitoring staff as to personnel's ingress and egress throughout the facilities.
- b. **Access Control Badge** - An identification badge that enables programmable access to secure entrances.
- c. **Access Control Reader** - A device that controls access and detects authorized personnel moving in and out of secure areas by reading an Access Control Badge and permitting or denying entrance based on privilege.
- d. **Agency** - A department, commission, board, or institution of the State of New Mexico.
- e. **Contractor** - A person or company under contract to provide goods or services to an Agency.
- f. **DoIT IT Resource Users** - All DoIT employees, contractors, vendors, consultants, temporary staff, seasonal staff, and any other users of DoIT IT resources.
- g. **Security Access Application** - A form used to request access to DoIT facilities.
- h. **Secured Area** - Any area with access restricted by Access Control Readers.

Physical Access Control Policy – DoIT-361-713

- i. **Physical Security Staff** - Physical security officers and managers.
- j. **Tailgating** - Also known as “Piggybacking,” the practice of intentionally or unintentionally following an authorized user to gain access to a Secured Area without using an AccessControl Badge.
- k. **Temporary Access Control Badge** - A Day access badge worn by a DoIT visitor or employee who has forgotten, lost, or misplaced their Access Control Badge.
- l. **Visitor** - An individual who DoIT security has signed into a DoIT facility and must be escorted and sponsored by DoIT staff throughout their visit while on the premises.

5. POLICY

Physical access to DoIT’s computer facilities, server rooms, and any work areas containing sensitive information must be physically restricted by way of Access Control Systems to individuals who have a legitimate business need for such access. Any individual needing physical access to DoIT facilities must be explicitly authorized by DoIT. Access authorization must be granted in accordance with the concepts of least privilege and separation of duties between job roles. DoIT may authorize temporary access for staff members, contractors, vendors, or visitors, and such temporary access shall only be granted on a case-by-case as-needed basis.

Before entering any DoIT facilities, individuals are required to identify uniquely and positively. Visitors must be easily distinguishable from onsite personnel. Visitors must sign the security register and be always escorted by an authorized staff member. If visitors bring equipment for maintenance tasks, tools should be presented to authorized staff members for verification. A visitor log must document the visitor’s name, associated entity, signature, date of access, entrance time, exit time, purpose of visit, Temporary Access Control Badge number, and authorized personnel escort. DoIT must retain the visitor log for a minimum of ninety (90) days. Removal of equipment from DoIT facilities must follow the *IT Change Management Policy* for documented approval.

Individuals with authorized access are not permitted to allow unknown or unauthorized persons to access Secured Areas, including by way of Tailgating.

Physical access to all DoIT facilities must be controlled by an Access Control System, *e.g.*, Access Control Readers and door locks. All doors to DoIT’s computer facilities must be always secured. If a door must be propped open (*e.g.*, when moving equipment, furniture, or supplies), the entrance must be continually monitored by an authorized employee. Surveillance equipment must be placed around sensitive areas throughout DoIT facilities.

Individuals with Access Control Badges that have been lost or stolen, or are suspected of being lost or stolen, are required to report the loss/theft to the Physical Security Department or manager immediately.

Network access to unused network jacks in public areas must be disabled.

Display screens that handle sensitive or valuable information must be positioned to not be viewable by unauthorized individuals (*e.g.*, from public windows, doors with windows, waiting areas, etc.).

6. ROLES AND RESPONSIBILITIES

a. DoIT CIO and CISO

The DoIT Chief Information Officer (CIO) is responsible for determining who shall have access to sensitive and protected information resources within DoIT. Access privileges shall be granted by the CIO in accordance with the user’s role and job responsibilities in the Agency. The DoIT Chief Information Security Officer (CISO) or CIO designee will ensure development, implementation, documentation, updates, and distribution of information as necessary to ensure the physical security of information assets.

Physical Access Control Policy – DoIT-361-713

b. Physical Security Manager

The Physical Security Manager will monitor physical security systems, ensure enforcement of physical security, and oversee a current list of authorized personnel.

c. Physical Security Staff are responsible for:

- i. Developing and maintaining a list of current personnel with authorized access to DoIT facilities;
- ii. Granting authorization and credentialed keys only when explicitly approved by upper management;
- iii. Reviewing and approving access lists and authorization credentials every thirty days at a ~~nimum~~ and
- iv. Removing access immediately in case of employment, vendor, contractor, or termination changes.

7. EXCEPTIONS

The DoIT CIO or CISO must approve in advance and in writing any exceptions to this Policy.

8. VIOLATIONS OF POLICY

Any DoIT IT Resource User found to have violated this Policy may be subject to disciplinary action, up to and including termination of employment.

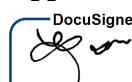
9. REFERENCES

- a. NMAC 1.12.20;
- b. National Institute of Standards and Technology (NIST) Publication SP800-53 r4: MA-2, MA-3(1), MA-3(3), MA-6(1), PE-1, PE-2, PE-2(3), PE-3, PE-3(1), PE-5, PE-6, PE-6(1), PE-6(2), PE-6(3), PE-6(4), PE-8, PE-16.

Physical Access Control Policy – DoIT-361-713**10. CHANGE HISTORY**

Date	Version	Changed By	Change Comments
09/30/2019	1		Initial Draft
09/30/2020	2		Revision Draft
02/26/2021	3	Raja Sambandam	Revised and routed for Union approval
05/21/2021	4	Olga Serafimova, Esq.	Reviewed and revised for legal compliance
09/20/2021	5	Olga Serafimova, Esq.	Final review and editing
5/5/2022	6	Brenda Fresquez	Reviewed for quality assurance
11/13/2023	6.1	Brenda Fresquez	Annual Review; updated header and footer
11/13/2023	6.1	Bryan E. Brock	Annual Review - Legal. No changes recommended.

Approval

DocuSigned by:

 437214FBE82C453...

Raja Sambandam, Acting Cabinet Secretary

11/14/2023

Date