Department of Information Technology

TITLE: *Physical Access Policy – Simms Building*	ISSUE DATE: March 23, 2012 EFFECTIVE DATE: March 23, 2012 REVISED DATE: March 6, 2017 NEXT REVIEW DATE
1. POLICY NUMBER: ***DOIT-773-3102-001-A 2012***	

1. AUTHORITY:

1.1. Department of Information Technology Act HB959, Sections 6-E3, 6-H1

1.2. The International Code Council (ICC) and National Fire Protection Association (NFPA) provides two fire codes, some of which have been adopted by the Santa Fe Marshal Office (SFMO) to assure standardization of life safety concerns. The two primary codes adopted are the ICC International Fire Code 2003 for new construction and NFPA Fire Prevention Code -1 and the 1997 life safety code - 101 for existing facilities.

2. REFERENCES:

2.1. Statewide Standard, Personnel Security S-STD-011, Section 4, Standard (OCIO)
2.2. B. State Personnel Board Rule, 1 NMAC 7, 11 Discipline
2.3. FEMA- Emergency Management Institute Training.
2.4. State Personnel Board Rule, Tile 1 NMAC Chapter 7, Part 11 Discipline

3. PURPOSE AND SCOPE

3.1. Assure a secure environment for all services provided by DoIT; that will protect against unauthorized access, detect attempted access and activate an effective response. Overall physical security needs may be assessed with regard to hardware, software, and enterprise infrastructure which includes voice, data, and radio services within the Simms Building and other DoIT facilities. The Department of Information Technology Data Center Facility Management(DCFM) has developed a Physical Access Policy to ensure a safe environment for confidential data and the staff that maintains it.

3.2. The Department of Information Technology has developed this policy to comply with federal and state statutes, regulations and policies of the agencies it serves.

4. DEFINITIONS

4.1. Access Control System: An automated system that manages access to secure locations and has the ability to track, record, and alarm.

4.2. Access Control Badge: An identification badge that has programmable access to secure entrances.

4.3. Access Control Reader: An intelligent device that detects authorized personnel in and out of secure areas quickly by reading an Access Control Badge.

4.4. Security Access Application: A Security Access Application is used to request access to the Department of Information Technologies facilities and Data Centers.

4.5. Agency: A department, commission, board, or institution of the State of New Mexico.

4.6. Building: John F. Simms Building, 715 Alta Vista, Santa Fe, New Mexico, 87505.

4.7. CIO: Chief Information Officer.

4.8. Contractor: The term "contractor" means an individual for whom the Department of Information Technology (DoIT) has registered and approved to work at Department of Information Technologies facilities.

4.9. Custodian: A GSD/FMD employee assigned to perform maintenance and janitorial services at a DoIT facility.

4.10. Data Center Facilities Management**:** DoIT Office of Security and Facilities Management that is responsible for maintaining a secure business environment through policy development and enforcement.

4.11. DoIT: Department of Information Technology.

4.12. DoIT Facility: John F Simms Building at 715 Alta Vista in Santa Fe New Mexico 87505

4.13. Enterprise Data Center: Simms Building facility that is used to house computer systems and associated components, such as telecommunications and storage systems.

4.14. Emergency: A situation or occurrence of a serious nature, developing suddenly and unexpectedly, and demanding immediate action.

4.15. Facilities Management Division (FMD)

4.16. Long Term: More than thirty days

4.17. Remote Data Center(s): Facilities within the Tiwa Building at 300 Broadway in Albuquerque New Mexico and 300 Don Gaspar in Santa Fe New Mexico. that is used to house computer systems and associated components, such as telecommunications and storage systems.

4.18. Staff: The term "staff" means all State of New Mexico employees that are assigned to the John F Simms Building.

4.19. Secured Areas**:** Locations in the Simms Building that are restricted with Access Control Readers.

4.20. Security Control Station: Security Control Station located in the front of the Simms facility. Houses Access Control and Video monitoring equipment along with day to day Security operations.

4.21. Security Staff: Physical security officers and Manager.

4.22. Tailgating: The practice of following a valid user through an open door without using an access control badge.

4.23. Temporary Access Control Badge: A Day Pass badge that is worn by a DoIT employee who has either forgotten, lost, or misplaced their Access Control Badge.

4.24. Visitor: The term "Visitor" means an individual for whom the DoIT security has signed in to be escorted and sponsored by staff.

5. POLICY:

5.1.1. **Overview** The Department of Information Technology will operate the State of New Mexico Data Center in compliance with:

5.1.1.1.1. All state and federal laws, rules regulations.
5.1.1.1.2. All state and federal laws policies
5.1.1.1.3. All best known practices as defined by DoIT
5.1.1.1.4. All City of Santa Fe applicable regulations such as, but not limited to building codes and fire prevention codes.

6. **PROCEDURES: Tasks required to ensure full compliance with this policy will be accomplished through Authorization, Authentication, Accounting and Enforcement.**

6.1. Authorization:

6.1.1. Authorization will be controlled by the DoIT DCFM. All authorization will require the approval of the manager of DoIT DCFM. All agencies have the right to require addition

authorization. For example agencies may require a signature from their CIO or senior IT manager

6.1.2. The DoIT DCFM will only authorize support personnel and contractors whose job responsibilities require access to the facility.

6.1.3. State Host agencies can obtain authorization for employees, contractors and visitors to limited or unobstructed access to the assets of their own agencies. No agency can authorize access to the assets of another.

6.1.4. Authorization of emergency access will only be granted by the manager of DoIT DCFM or a representative of the agency designated at the time of authorization.

6.2. Authentication:

6.2.1. Access to the Simms building will be authenticated by pictured badge.

6.2.2. No badge may be loaned or borrowed.

6.2.3. Visitors will by authenticated by a pictured ID issued by a government or municipality such as a driver license, passport etc.

6.2.4. Lost or stolen badges must be reported immediately. (within one hour) An employee that forgets or loses their access control badge must render a picture ID upon receipt of a temporary access badge.

6.2.5. Agencies are responsible for the integrity of their list of authorized personnel. They must notify the DCFM immediately (within one hour) in the case of termination of an employee it is the responsibility of the agency's Human Resources (HR) Office to promptly notify the DoIT DCFM of an employee's separation or termination of employment. The HR Office is responsible for assuring that the Security Access Badge is returned to the DCFM.

6.2.6. A contractor supporting a host agency reports to host agency a change of roles or responsibilities is needed within 24 hours.

6.2.7. DoIT will reserve the right to deactivate badges due to lack of use. (The time period for this procedure is deliberately omitted for security purposes). Employees that only use their badge on rare occasions should notify the DCFM of this situation.

6.3 Accounting

6.3.1 DCFM will maintain a record of who is authorized and all personnel that have been authorized by their supervisor.

6.3.2 Photo and authorization records of authorization will be available to the front desk Security staff for immediate access control.

6.3.3 DoIT will provide assistance to all federal agency audits and incident response. Agencies are responsible for notifying the DCFM of recording responsibilities such as length of retention etc.

6.3.4 On site security officers will keep a log of all events. Logs will be kept on the last 5000 occurrences to date.

7.1 Enforcement

7.1.1. Access will be granted through the use of a Security Access Application form.

7.1.2 Forms will be signed by the manager of the DCFM and the Agency sponsor. Forms will be retained by the DCFM.

7.1.3 All personnel requiring access to the data center will be fingerprinted.

7.1.4 Contractors and agencies will be issued a badge of a different color for easy identification of limited access.

7.1.5 Infrequent visitors such as contractors may be asked to surrender a driver's license upon arrive and sign out a badge at the security officer's discretion.

7.1.6 Visitors to remote locations may sign out keys and badges without surrendering a driver's license based on prior approval by the manager of the DCFM.

7.1.7 Access will be permitted by presentation of a micro chipped badge to a badge reader. The reader will unlock various doors based on the authorization of the individual.

7.1.8. Attempts to by-pass security systems such as "tailgating" will be thwarted by on site security staff.

7.1.9. On site security staff will be supported by the state police.

7.1.10. All personnel will display badges in a clear view and worn above the waist. Badges will not be obscured by clothing or attire.

7.1.11. Access is permitted between the hours of 6:00 am. and 5:30 pm. Monday through Friday. Weekend access is limited authorized personnel that have been granted weekend access privileges

7.1.12. Visitors must be authorized and escorted by authorized employees. Visitors that are found without an escort will be escorted off the premises. Sponsors that have left visitors unescorted will have their badges deactivated until an explanation has been made. The explanation will be logged in the daily security log.

7.1.13. Visitors must be authorized and escorted by authorized employees.

7.1.14. DoIT DCFM shall comply with The International Fire Code as adopted by the State of New Mexico, Fire Marshal's Division Section 404.1-404.3.1 by exiting the building immediately when directed by an alarm Security Staff. All agency and contracted support staff will also comply by following the direction of their sponsor and the on-site security officers.

7.1.15. DoIT security staff will assist deaf and disabled persons requiring assistance with access or compliance such as response to alarms. Sponsors are responsible for identifying special needs.

7.2 Equipment Accountability

7.2.1 DoIT DCFM will maintain an active anti-theft program therefore will require the right to detain anyone leaving the premises with equipment of any type.

7.2.2 In the event of any removal of equipment DoIT DCFM will photograph all personnel leaving the premise and the equipment being removed.

7.2.3 DoIT DCFM will provide video surveillance of the premises including all agency equipment racks.

7.2.4 DoIT DCFM will provide videos on portable media for at least the previous 45 days. In order to preserve chain of custody for evidence in a criminal trial or hearing The DCFM will require a request in writing. The DCFM recognizes the state encrypted email system as a valid signature request.

7.2.5 Request for video over the state email system will be honored within 24 hours.

7.2.6 DoIT will maintain a chain of custody for all evidence

7.2.7 In the event of any installation of equipment DoIT requests that a ticket be opened with the Enterprise Helpdesk. This can be used as documentation of changes to the inventory.

7.2.8 DoIT request but does not require copies of agency inventory in order to better protect your agency from theft.

7.2.9 Each reported infraction of this policy will be handled on it's own merit and may be subject to disciplinary action in conjunction with the State Personnel Board Rule, Title 1, NMAC Chapter 7, Part 11, Discipline.

7.2.10 The DCFM will review this policy annually in accordance DoIT policy client agency needs.

APPROVAL:

_____ _____

Daryl Ackley, Secretary Date
Department of Information Technology

Appendix A : Acknowledgement Form

Before signing the security access application all personnel will read this summary of acknowledgements.

All persons who are granted access to the John Simms building are required to obey all laws, rules and policies of the State of New Mexico and the Department of Information Technology (DoIT) as well as federal laws and rules and policies of federal agencies.

By accepting of the any level of access you are hereby agreeing to the following:

1. No one is allowed to ever lend a badge.
2. No one is allowed to ever borrow a badge.
3. Lost badges must be reported immediately
4. All persons entering in or on state property are prohibited from soliciting, requesting or receiving political donations.
5. No solicitation materials may be posted.
6. Smoking is not allowed within 30 feet of the building.
7. Solicitation of charitable contributions is only allowed by prior authorization. This requires prior authorization and proof on non-profit status.
8. Activates of labor union permitted by agreement will be allowed and respected.
9. No firearms or weapons of any type are allowed within 30 feet of the building.
10. All violations observed shall be reported to the security desk.
11. All persons will be held to any and all other laws, rules and policies put into effect after the posting of this message.

Statutory authority is granted by the following State of New Mexico Administrative Codes
[1.5.24] N.M.A.C
[1.5.22.8] N.M.A.C
[1.5.21] N.M.A.C

I have received, read, and understood the **Policy:** ***Policy Title*** **DOIT-773-3102-001-A.** I understand it is my responsibility to adhere to this policy. Should I have any questions I will notify the DoIT Physical Security Office (505) 827-2116.

Printed Name	Signature

Agency/Company

Title _____ Date (mm/dd/yyyy) _____