DEPARTMENT OF HUMAN SERVICES

Building Access and Control Policy

Description:

This policy establishes controls for physical access to Department of Human Services (DHS) Central Office locations. Central Office locations can contain a variety of confidential and/or protected information related to the services DHS provides. The business of the agency can requires business need only access to Federal Tax Information (FTI), Social Security Information (SSI), and information from Criminal Justice Information Systems (CJIS) data.

Reason for Policy:

Federal and State statues, rules, regulations and guidelines require that access to areas containing non-public information must be protected. Central Office locations can contain a variety of confidential and/or protected information related to the services DHS provides. The business of the agency requires business need only access to Federal Tax Information (FTI), Social Security Information (SSI), and information from Criminal Justice Information Systems (CJIS) data.

Employee safety concerns may also require regulated entry into their work area. To meet these needs, DHS Central Office Physical Security works with designated department representatives to accurately assign and maintain badge access rights to the facility. Access rights on each badge must be accurately programmed based on agency security needs, building access trend measures, and minimum access necessary to perform essential job functions to meet authorized individuals' business needs. Badge access is limited to DHS employees, MNIT partnering with DHS employees working on applications or projects that support DHS work, state associates and approved, escorted contractors.

Badge access card programming will be based on:

• Agency security needs, building access trend measures, and minimum access necessary to perform essential job functions; and

• Physical access controls required under Federal Tax Information (FTI), Social Security Information (SSI) and Criminal Justice Information Systems (CJIS) data guidelines.

This policy will establish the necessary access control standards to 1) allow DHS Physical Security to maintain appropriate security measures in the facility; and 2) provide guidelines for supervisors and sponsors requesting

appropriate badge access card programming for each authorized individual requesting access to secured workspace.

Applicability:

This policy and its procedures apply to all employees, contractors, volunteers, external auditors, interns and any individuals having access to DHS physical workspace, data and systems.

Failure to Comply:

Failure to comply with this policy and its procedures may result in disciplinary actions, including termination, suspension of contractor access or cancellation of contracted services.

Policy

All badge access cardholders must present their badge access card to a badge reader and be granted access by the access control system to enter a secured area.

Monitored access permissions include who may enter and when and where they can access the secured area in the facility. DHS Central Office Physical Security maintains an Authorized Access List database that is audited via bi-weekly report, annually overall and as needed when a badge holder changes employment within the agency, leaves the agency or otherwise has a change in badge access rights.

Access assignments for individuals are based on the following:

- **DHS and MNIT partnering with DHS Employees:** Standard "basic" access to 444 Lafayette and/or Elmer L. Andersen Building protected areas are programmed for all authorized employees at time of hire on the first formal date they are authorized to start work when all security and organizational requirements have been met. Time frames for admission are based on the Department of Minnesota Management and Budget and the applicable Bargaining Agreements definition of a work day. Currently, this time period is Monday through Friday from 6 a.m. to 10 p.m. and Saturday/Sunday 6 a.m. to 6 p.m., excluding State-designated holidays.
- **Contractor** badge access will only be programmed for times and areas essential to the completion of their contracted work when DHS employees are present to provide an escort.
- **Individuals** working in the 444 Lafayette or the Elmer L. Andersen Building will not be programmed for access into other St. Paul Central Office sites unless a business need is identified and requested through an Access Change Request.
- **Afterhours access** shall be limited only to employees who have job responsibilities requiring non-business hour entries. Responsibilities that would typically meet this criteria include:
    - Facilities and physical security staff associated with physical response and recovery efforts related to priority 1 and 2 functions

    - Individuals responsible for maintaining critical infrastructure and data systems associated with priority 1 and 2 functions
    - Individuals who support DHS legislative functions during the session whose work is deemed essential by their work unit director, Assistant Commissioner, Deputy Commissioner or Commissioner for afterhours access
    - DHS executive staff who are responsible for essential agency work and approved by an Assistant Commissioner, Deputy Commissioner or Commissioner for afterhours access
    - Emergency responders to building events that could impact DHS business or employee safety
- **Employee family members, personal care assistants and guests** are only authorized into secured work areas when registered as a visitor and escorted by a DHS or MNIT partnering with DHS employee. Family members and guests will only be permitted into secured areas during normal business hours, Monday through Friday, 8:00 a.m. to 4:30 p.m., excluding State-designated holidays. Family members and guests who are not registered as visitors of DHS or MNIT partnering with DHS state employees will not be permitted entry into secured areas.
- **DHS work associates** with badge access to secured work locations require a DHS employee supervisory sponsor. See the Associate Badge Access Standard Practice for more information on associates.
- **DHS privacy training**: DHS employees, contractors, volunteers, external auditors, interns and any individuals having access to DHS data and systems, must comply with the training requirements in the DHS Protecting Not Public Data Policy. Failure to complete required training in the DHS Protecting Not Public Data Policy will lead to the suspension of access to DHS Central Office facilities upon notice from the DHS Information Privacy Office.
- **DHS Privacy Training Exemption**:
  Individuals who may be exempt from the DHS privacy training include:
    - Officers of the court
    - Federal or State auditors
    - Other individuals approved by the DHS Information Privacy Office who may have credentials that meet, exceed or may be exempt from DHS policy standards
- DHS work associates or policy unit contractors without access to the DHS network or assigned workstation are considered visitors. Access to DHS meetings located in secured areas is arranged by the meeting host through the required InfoLink visitor registration process and Information Desk.
  See Meetings and visitors on InfoLink.
- Badge access cards not used by individuals programmed into the DHS access control system within a 365-day period are suspended.
- Contractors performing facility or equipment maintenance are granted access as follows:
    - Facility maintenance contractors (plumbers, carpenters, electricians, etc.) who are required to be on-site for several days are subject to criminal background checks by DHS Physical Security. Upon clearance, workers are required to complete a DHS Confidentiality Agreement prior to being issued a limited access badge.
    - Short term facilities maintenance or equipment technicians are required to register as a visitor and escorted by appropriate DHS staff while in areas containing non-public information.
- All badge access cardholders must present their badge access card to a badge reader and be granted access by the access control system to enter a secured area

Procedures

I. Standard Building Access

All badge access cards (also known as ID cards, key cards, or badges) are programmed with standard "basic" access to DHS Central Office locations: Monday through Friday, 6 a.m. to 10 p.m., and Saturday/Sunday, 6 a.m. to 6 p.m., excluding State-designated holidays. Further badge access must be formally requested through an Access Change Request. Access Change Requests are reviewed based on agency security needs, building access trend measures, and minimum access necessary to perform essential job functions.

II. Non-Standard Building Access

- See Policy section above for outline of permitted access, including non-standard building access.
- Badge access cards with additional Personal Identification Number (PIN) access have their PIN codes changed annually on the first Monday in July at the start of the new fiscal year. Request for PIN changes (annually or as needed when a badge holder changes employment within the agency, leaves the agency, or otherwise has a change in badge access rights) are documented through an Access Change Request. Once the Access Change Request is approved by the supervisor and reviewed by a member of DHS Central Office Physical Security , the PIN will be logged and updated in the access control system using a random number generator. The new PIN will be provided to the badge holder via a secure means of transmission. Standard notice language with the PIN includes the following:
    - As an employee with a badge requiring additional PIN access, your PIN code is automatically updated the first Monday in July at the start of the new fiscal year.
    - Keep this PIN secure. Do not share your PIN or record it in an unsecured location, like in a pencil drawer or on a piece of paper under the keyboard or desk.
    - If you believe your PIN has been compromised, contact the Security Desk using the number on the back of your badge, (651) 431-3000, and ask to be routed to a member of DHS Central Office Physical Security.

III. Building Access Change Requests

- For new hires, badge access card programming begins with the employee onboarding process. All new employees are given "basic" access which is Monday through Friday, 6 a.m. to 10 p.m., and Saturday/Sunday, 6 a.m. to 6 p.m., excluding State-designated holidays.
- Requests for building and secured work area access beyond the "basic" level requires an Access Change Request approved by the employee's supervisor.
- An Access Change Request can be submitted by the employee themselves, supervisor of the employee, or manager. The Access Change Request needs to be approved by the employee's supervisor or manager with final review by the DHS Central Office Physical Security. If approved by the DHS Central Office Physical Security, the minimum necessary access levels are programmed onto the employee's access badge.

- Special requests for short term extended access privileges to meet weekend or other work flow demands must be approved by the employee's supervisor for review through the Access Change Request. Approvals or requests to modify access levels into DHS facilities must be submitted using the Access Change Request, which includes the names of employees, times, dates and locations of requested access. See DHS Physical Security on Infolink.
- Building access requests for associates (individuals from other state government agencies) and program unit contractors are also submitted using the employee onboarding process. See Buildings, facilities on Infolink. All associate, interns and contractor badge access requests must include an expiration date and identification of a DHS sponsor. Associate access requests need to meet Associate Badge Access Standard Practice and are reviewed every six months to ensure badge access is still required.
- DHS sponsors of a contractor, auditor or board member are responsible for ensuring that individual's access is at a minimum level. Sponsors are required to alert DHS Central Office Physical Security of any status changes of the individual such as early termination of a contract or internship or resignation of a board appointment. The sponsor or the appropriate Technology Support Liaison (TSL), must ensure Remedy notifications have been completed.
- Badge access cards not used within a 365-day period are suspended. Reactivation of suspended access badges will require review and approval by the business area prior to reactivation by DHS Central Office Physical Security.

IV. Requesting Replacement Badge or Reporting Lost or Stolen Badge

- **Request a replacement badge** online using the Badge Replacement Request. The Badge Replacement Request form can be used to request a name change, photo update, or report a lost or stolen badge.
- **Name changes** occur in two separate processes:
    - **Email and Microsoft Teams name changes** are requested through **Human Resources.**
    - **For name change on a badge,** the legal name (name listed in Sema4) is on the back of the badge and the preferred name is on the front of the badge. Use the Badge Replacement Request to submit a name change.
    - **Requested name changes should not violate policies in place for state employees. For more information on the process for change of legal name, see Minnesota Judicial Branch – Name Change.**
- **Lost or stolen badges** should be reported immediately via the Badge Replacement Request or by notifying security at (651) 431-3000. The lost or stolen badge is then deactivated by security to prevent the badge from being used by unauthorized parties.
- **Badge photo updates** are required once every seven (7) years. Employees can upload a photo to the Badge Replacement Request form. The picture requirements are the same as a passport photo: In color; taken in full-face view directly facing the camera; and no decorative borders, colors, or filters.

Related Policies and References:

- DHS Protecting Not Public Data Policy

Legal Authority:

- Centers for Medicare & Medicaid Services, Harmonized Security and Privacy Framework-Exchange Reference Architecture Supplement
- Health Insurance Portability and Accountability Act of 1996
- IRS Publication 1075 (PDF)
- Minnesota Data Privacy Act

Standards:

- Associate Badge Access Standard Practice
- DHS Central Office Physical Security Standard Practice

Definitions:

Associate: Employee of a state agency other than DHS which requires access for DHS Central Office directly related to DHS business needs. See Associate Badge Access Standard Practice on SharePoint.

Authorized Access List (AAL): List maintained in access control database of DHS employees, MNIT partnering with DHS employees and non-DHS personnel who have a frequent and continuing need to enter a restricted area, but who are not assigned to the area. The AAL contains badge holder's name, department name, name and phone number (if assigned) of the supervisor or sponsor authorizing access, address of assigned work location, purpose and level of access.

Badge Access Card (also known as ID cards, key cards, or badges): Physical or electronic pass issued by DHS Central Office Physical Security Team. Badge access cards are programmed with specific permissions for accessing exterior and interior physical building space. Permissions assigned to the badge access card are based on agency security needs, building access trend measures, and minimum access necessary to perform essential job functions.

Building Access Trend Measures: Reports using DHS Central Office Physical Security badge access card and registered visitor data. Badge access card data is not public security information under Minnesota Statutes, section 13.37.

Business Hours: Business hours for Central Office locations open to the public are Monday through Friday, 8:00 a.m. to 4:30 p.m., excluding State-designated holidays. The exterior doors for locations open to the public are locked and badge access only prior to 8:00 a.m. and after 4:30 p.m., Monday through Friday. The exterior doors

of Central Office locations not open to the public are locked and badge access only 24/7. All exterior doors of Central Office locations are locked and badge access only all day Saturday, Sunday, and observed State Holidays.

Chief Administrative Officer (CAO): State employee assigned by their Assistant Commissioner to coordinate activities throughout the organization and maintain administrative continuity throughout the various work units.

DHS Central Office Locations: State-owned or leased office buildings that support the work of DHS as an executive branch agency responsible for administration of programs and services for the people of Minnesota.

- Lafayette Building, 444 Lafayette Road North, St. Paul, MN 55155
- Elmer L. Andersen Human Services Building, 540 Cedar Street, St. Paul, MN 55101
- Distribution Center 1/Issuance Operations Center (DC1/IOC), 355 E. Eighth Street, St. Paul, MN 55101
- Brainerd Building 20, 11630 State Avenue, Building #20 MN-309, Brainerd, MN 56401

The MNIT EDC1 location is leased separately by MNIT from the Department of Administration and is not a part of DHS Central Office workspace.

DHS Central Office Physical Security: Management Services Division staff responsible for maintaining compliance with established security standards and enforcing physical access authorizations at entry/exit points to Central Office facilities by 1) verifying individual access authorizations before granting access to the facility; 2) controlling ingress/egress to the facility using physical access control systems/devices or guards; 3) maintaining physical access audit logs for entry/exit points; 4) providing security safeguards to control access to areas within the facility officially designated as non-public and public accessible; 5) reinforcing the agency requirement to escort visitors and monitor visitor activity; 6) securing keys, combinations, and other physical access devices; 7) maintaining inventory physical access devices; and 8) auditing and updating combinations, keys and building access when an employee retires, terminates employment, or transfers to another position.

DHS Commissioner: State employee appointed by the Minnesota Governor (and subject to confirmation by the Senate) who serves as the head of a department.

DHS Deputy and Assistant Commissioners: State employees appointed by the DHS Commissioner.

DHS Employee: State employee who reports directly or indirectly to the DHS Commissioner.

Director: Individual designated by Human Resources as a director.

MNIT Partnering with DHS Employee: State employee who reports directly or indirectly to the MNIT partnering with DHS Chief Information Officer, works on applications or projects that support DHS work, and has an assigned physical or telework work location within a DHS Central Office facility. MNIT employees who do not report directly or indirectly to the MNIT partnering with DHS Chief Information Officer, are not assigned to a DHS Central Office physical or telework work location, or pass through DHS to access MNIT EDC1 at Andersen, are not considered MNIT partnering with DHS employees.

Personal Identification Number (PIN): A number assigned to an individual used to authenticate a user accessing a system.

Policy Unit Contractor: An individual hired by the Department for a designated period of time to complete a project, research or assignment for a policy related to a division. These individuals are not members of any trades such as carpenters, plumbers, painters, etc.

Supervisor: Individual responsible for developing position descriptions of various work duties including the minimum necessary physical building or area access requirements to complete the assignments. Upon hiring of new employee or reassignment of an existing employee complete the required onboarding process to initiate new badge access.

Policy Contacts:

Name: Jennifer A. Smith; **Email:** Jennifer A. Smith; **phone:** 651-431-2207

Policy History:

Issue Date: 10/11/2024
Effective Date: 10/11/2024

Version 4.0

03/26/2024

Version 3.0
06/02/21

Version 2.0
05/15/17

Version 1.0
08/27/2013 (Initial Release)

This policy and its procedures remain in effect until rescinded or updated.