



**Maine State Government
Dept. of Administrative & Financial Services
Office of Information Technology (OIT)**

OIT Data Center Access Control Procedure

I. Statement

It is the responsibility of the Enterprise Operations and Monitoring (EOM) section of Core Technologies Services (CTS) to provide a secure, stable physical environment for servers and mainframes.

II. Purpose

The purpose of this document is to clarify the process by which employees, contractors, vendors, and other individuals are authorized for access, and the conditions for controlling that authorized access. EOM must be able to guarantee that the physical environment is maintained and operated in a professional manner equivalent to what one would expect of a commercial facility.

III. Applicability

This procedure applies to access to OIT Data Centers. This procedure must be adhered to by any and all persons who may have occasion to enter these Data Centers for any reason.

IV. Responsibilities

- A. Data Center Visitors: Data Center Visitors are responsible for complying with this procedure.
- B. Enterprise Operations and Monitoring: EOM staff and management are responsible for implementing, monitoring, and enforcing this procedure.
- C. OIT Management: OIT management is responsible for maintaining a list of employees and contractors who have passed the Maine State Police Background check and who also have work duties which require a physical presence in a Data Center.
- D. Security: Security Officers (contract security staff) are responsible for monitoring access requests under the RFC process as detailed in this procedure.
- E. Supervisory Personnel: Managers and Supervisors are responsible for enforcing procedure compliance by Data Center Visitors under their supervisory control.

V. Directives

A. General procedures regardless of access level:

1. All persons, regardless of their method of entry, must make a log entry in the log book inside the OIT Data Centers listing all of the following:
 - a. their name

- b. a description of the reason for their entry, a Request for Change (RFC) number, an EOM Project footprints ticket number, or a Customer Support Project Footprints Ticket number
 - c. the date and time of their entry
 - d. the date and time of their departure
2. Handwriting will be legible and narratives will be sufficiently descriptive to indicate the nature of the problem being worked on. Log entries such as “Server”, “GIS”, “Network”, or “Service” are not acceptable and will be reported to management as a violation.
3. ALL personnel are required to use their access card at the card reader outside the Data Center when entering the Data Center, including when in a group, and even if their card is not authorized to grant access. The action will be automatically recorded in the access control system log files and can be compared to the sign-in book if necessary.
4. Personnel are expected to notify Facility Services in advance of any known electrical needs, physical server changes, or any other action involving the electrical power system or physical connection to the network through the use of a footprints ticket under the OIT Facilities project (Work Order) or the OIT Change Management Project (RFC) as appropriate. Personnel must not plug equipment into any connection or make any other physical changes without authorization from Facility Services personnel as recorded in these tickets, as a circuit overload may result.
5. All visitors without access privilege will be escorted by authorized personnel.
6. Authorized staff members will be totally responsible and held accountable for an escorted individual’s or group’s actions at an OIT Data Center.
7. On occasion (e.g., weekends when there may be only one individual on duty), the Data Center may be unstaffed for a short period of time for breaks. During these ‘after hours’ times, the operators will carry a cell and/or pager. The contact number(s) will be posted on the wall just above the ‘Sign-in Book’ inside the Data Center.
8. Anyone responding to an automated contact by WEBNM or some other form of ‘call home’ system must follow procedures as outlined in this document.
9. If Standard Operating Procedures (SOP) are not sufficient to resolve a given situation, then escalation will be initiated based upon the [Duty Roster](#)¹.

B. Specific Guidelines and Procedures

1. 24/7 Access (24 hour access 7 days per week) procedures:

- a. Permanent 24/7 access permission is reserved for EOM, Security Officers and personnel authorized by supervisors. All other persons are considered Data Center Visitors.

¹ <http://csn.state.me.us/login.php>

2. Daytime access (6 AM – 6 PM Monday through Friday, No Holidays):

- a. Management will select a limited list of staff members for Data Center support between the hours of 6 AM to 6 PM, in order to keep the large number of personnel down to a controllable number.
- b. All other personnel needing access to any Data Center must be escorted by staff having an authorized entry card.

3. Off-Hours and Emergency Access (6 PM to 6 AM Monday through Friday, Holidays, and weekends):

Off hours access to Data Centers are subject to the following:

- a. Name must appear on a pre-approved 24/7 list such as the OIT Duty Roster or EOM Organizational Chart,
- b. or, be escorted by staff on a pre-approved 24/7 list,
- c. or, reference an OIT Change Management project Request For Change (RFC) number. (See **OIT Change Management RFC** procedure below)
- d. or, have an Authorizing Agent (see definition below) notify EOM Duty Operator of access approval to OIT Data Center (See **Emergency Access Customer Support Ticket** procedure below)
- e. Emergency access will be granted for a maximum of 24 hours only. If access is required beyond that, the task should be transferred to an emergency RFC.

4. Pre-Approval process (General):

- a. Individuals must pass a Maine State Police (MSP) background check as detailed in the [Physical Access Card Request Form for OIT Areas](#)² request form before they may be granted approval for badge access to OIT Data Centers.
- b. Supervisor approval is required for specific job duties requiring physical presence in the Data Center.
- c. Vendors, Contractors, outside Agency personnel and other visitors whose presence is regularly required to support Data Centers may be granted pre-approved access (see [Physical Access Card Request Form for OIT Areas](#)). Depending on the frequency of the access requirement, the individual may be issued a permanent badge. Individuals who are not pre-approved will be accompanied and escorted by pre-approved personnel.

5. Pre-Approval process (OIT Change Management RFC) – Security Staff Procedure

- a. RFC must include the beginning and ending dates and times of access as well as names of those requiring access.
- b. In order to enter or modify the dates and names, the user must select the appropriate Data Center.
- c. If the access begin and end times are the same or if the end time is before the begin time, access cannot be granted.
- d. Security staff will routinely monitor RFCs that are assigned to the OIT-Building-Access group. They will:
 - 1) Compare the names listed in the RFC against a list of individuals who have passed a MSP background check.

² <https://footprints.state.me.us/footprints/security.html>

- 2) Submit a request to Building Control Center (BCC) through their E-Logger system to apply the appropriate access level to the named individuals and the Start and End date/time of the access.
- 3) Update the RFC indicating the E-Logger log number.
- e. BCC staff will update the access for the requested individuals prior to the start time, and revoke the access after the requested end date/time.

6. Pre-Approval process (Emergency Access Customer Support Ticket) - Enterprise Operations and Monitoring Emergency Access Procedure

- a. EOM staff may approve OIT staff for Data Center access under the following conditions:
 - a. When an SOP requires them to call in support staff to respond to an incident.
 - b. When contacted by an authorizing agent (see definition below) who will approve support staff for emergency off hours Data Center access to respond to an incident.
- b. EOM Staff will create a Customer Support ticket or update an existing Customer Support ticket documenting the incident.
 - a. New tickets should be filled out as normal documenting the incident.
 - b. EOM Access Authorization section of the ticket must be completed on new and existing tickets (see SOP for authorizing access).
- c. EOM staff will submit an E-Logger request to building control to add the appropriate access level(s) to the requestor(s) card(s) (see SOP for submitting E-Logger).
- d. EOM staff will submit an E-Logger requesting removal of added access level(s) from the requestor(s) upon notification of ticket closure, or after 24 hours, whichever is less.

VI. Definitions

- 1. **Authorizing Agent** – An authorizing agent is an on-call responder, the on-call duty manager, or another OIT manager who can vouch to the EOM staff that a specific individual requires access to OIT Data Centers for a specific reason.
- 2. **Data Center** – A room managed by EOM for the purpose of providing optimal environmental, power, and security conditions for the operation of State of Maine critical information processing hardware.
- 3. **Data Center Visitor** – A Data Center visitor is any person who is not part of EOM, Security staff or an authorized employee and therefore does not have permanent 24/7 access to the Data Centers.
- 4. **Duty Roster** – A list of support personnel and Duty Manager who are responsible for addressing problems encountered with various OIT areas and systems when established Standard Operating Procedures (SOP) are insufficient to resolve the situation.
- 5. **EOM** – Enterprise Operations and Monitoring

VII. References

- 1. OIT Access request form: <https://footprints.state.me.us/footprints/security.html>

2. On-Call Duty Roster <http://csn.state.me.us/login.php> (You must log in with your AD credentials to access this information).

VIII. Document Information

Initial Issue Date: April 2, 2012

Latest Revision Date: July 13, 2015 – to update Document Information.

Point of Contact: Henry Quintal, Architecture-Policy Administrator, OIT, (207) 624-8836.

Approved By: James R. Smith, Chief Information Officer, OIT, 207-624-7568.

Enforced by: Kevin St. Thomas, Enterprise Security Officer, OIT, 207-624-9845.

Legal Citation: [Title 5, Chapter 163: Office of Information Technology](#)³

Waiver Process: See the [Waiver Policy](#)⁴.

³ <http://legislature.maine.gov/statutes/5/title5ch163sec0.html>

⁴ <http://maine.gov/oit/policies/waiver.htm>