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

OIT Office Complex Building Access Procedures

1.0 Purpose

It is the responsibility of the OIT Security Officer to provide a secure and stable physical environment. The purpose of this document is to clarify and delineate the process by which employees, contractors, vendors, and other individuals are authorized for access, and the conditions for controlling that authorized access.

2.0 Definitions

2.1 **Access Controlled Area**: Any area of the building which is secured by an access controlled door or key locked door.

2.2 **Building Complex**: The building and parking lot area.

2.3 **Business Visitor**: A Visitor to the facility who is here to meet with an employee to conduct business, such as attending a business-related meeting or performing work.

2.4 **Card Holder**: Any individual who has been issued a Personal Access Badge. A Card Holder may be an Employee, Contractor, or Intern.

2.5 **Normal Business Hours**: Normal business hours for the building are 6:00 a.m. to 6:00 p.m. (06:00 to 18:00) Monday through Friday, exclusive of scheduled state holidays and other shutdown days.

2.6 **Non-Resident Contractor**: Someone under contract to OIT, the building owner, or other State of Maine agency who has some need to access the facility but does not have a permanent assigned workspace at the facility. This includes contractors who are on-site at the facility for less than 11 consecutive working days.

2.7 **Non-Resident Employee**: Any State of Maine employee who has frequent or occasional need to access OIT Office Complex facilities but whose primary work location is not the OIT Office Complex facility.

2.8 **Off Hours**: Any time other than the above defined normal business hours.

2.9 **OIT High Security Areas**: These areas require special authorization for access. Visitors must always be accompanied while in these areas. Visitors who do not present valid photo ID must not be allowed any access to these areas.

2.10 **OIT Office Complex**: Currently the 51 Commerce Drive facility and the 45 Commerce Drive facility, in Augusta.

2.11 **Personal Access Badge, Personal Badge**: An access control badge issued to an individual for their exclusive use to enter the facility and any authorized access controlled areas of the building.

2.12 **Personal Visitor**: A Visitor to the building who is here visiting an individual or the building for a social purpose, such as having lunch, visiting a relative, attending a party, giving blood, etc.

2.13 **Policy, Access Policy, Access Control Policy**: This document may also be referred to as the Policy, the Access Policy, or the Access Control Policy.

2.14 **Resident Contractor or Intern**: A person contracted to perform work for OIT who is provided with a workspace at an OIT Office Complex. Resident Contractors or Interns maintain a work schedule and work habits that are like those of employees.

2.15 **Resident Employee**: Any State of Maine employee whose primary work location is an OIT Office Complex building.

2.16 **Visitor**: Any other person who is not an Employee, Contractor or Intern as defined above.

3.0 Applicability

These procedures apply to access to any *OIT Office Complex* and must be adhered to by all persons who may have occasion to enter a complex for any reason.

4.0 Responsibilities

4.1 Chief Information Security Officer: The Chief Information Security Officer (or designee) is responsible for enforcing these procedures.

4.2 OIT Office Complex Staff: Staff and management are responsible for implementing, monitoring, enforcing, and complying with these procedures.

4.3 OIT Office Complex *Visitors*: Visitors are responsible for complying with these procedures.

4.4 Security: OIT Office Complex Security Officers (contract security staff) are responsible for enabling and disabling access levels as detailed in these procedures or otherwise authorized by OIT Office Complex staff.

4.5 Supervisory Personnel: Managers and Supervisors are responsible for enforcing compliance by complex Visitors, employees, and contracted staff under their supervisory control.

5.0 Directives

5.1 **Any OIT Office Complex is a controlled access building.** The information, forms, and material handled at this facility are of the most sensitive and confidential

nature. Therefore, it is necessary to limit building access to those people who have a business reason to be there, or who are visiting a specific employee at the facility.

5.2 **Entry to the building must be recorded**. There must be a record maintained of persons who enter the building. This recording may be accomplished using a card access control system, a sign in log, video monitoring system, or other mechanism. No one will be admitted to any *access controlled area* of the building unless they use an authorized access control card, or sign a log and present identification credentials.

5.3 **Employees are responsible for all persons who visit them whether for business or personal reasons.** Employees must provide an appropriate level of supervision of Visitors so that security requirements are maintained. While it is not necessary for an employee to accompany a Visitor continuously, the employee must ensure the Visitor does not inadvertently compromise security or disrupt essential services. For example, it is not necessary to accompany a Visitor to the rest room, but the Visitor must be supervised while in the computer room.

5.4 **All persons in the building must prove identity, whether they are a building employee, contracted employee, or visitor.** Building employees and *Resident Contractors* will be issued a photo identification badge after an access request procedure is followed. Visitors and occasional contractors will be issued a temporary badge identifying them as a Visitor or contractor after presentation of proof of identity. Because employees, contractors, and authorized Visitors are identified, it will be easy to spot an unauthorized individual in the building. Persons who are unable to present proof of identity must be considered a security risk, and must not be allowed in high security areas.

5.5 **There are areas of the building that require a higher level of security.** Access authorization for these areas (such as computer rooms, Telco closets, test lab, etc.) is granted by the area supervisors, and administered by building security staff.

5.6 **Every employee has a responsibility to help ensure the security and safety of their fellow workers, and the building.** Although we have a security officer on duty 24 hours a day, and an access control system to prevent unauthorized access, every employee must take responsibility to ensure building security as well. Employees must not compromise building security by propping doors open or holding a door open to let someone in the building. Taking such actions lessens building security and increases the risk to every employee. Employees should feel empowered to challenge anyone in the building who is not wearing an identification badge to present their badge. Individuals who are unable to produce a badge must be immediately escorted to the security office to be authorized. Employees must also report to the security office any security irregularities such as doors left open.

6.0 <u>Procedures</u>

6.1 Access Control System.

6.1.1 Access to an OIT Office Complex is controlled using a card access system. This is a proximity card access system in which the access card is held near (about 2") to the reader. All access attempts, whether successful or failed are recorded and stored by the access control system. The system is managed by the Bureau of General

Services, Building Control Division.

6.2 Access Identification Badges – General.

6.2.1 All persons in access controlled areas must wear and display a valid ID badge issued in accordance with this Policy.

6.2.2 Areas not considered access control areas are those not secured by either a card access reader or keyed lock.

6.2.3 Employees must immediately escort persons found in access controlled areas without proper identification to the security office, or at a minimum, immediately notify the security office of such persons if they refuse to be escorted to the security office.

6.3 *Personal Access Badge* layout.

6.3.1 Badge layout – general.

6.3.1.1 The cardholder photo is in the upper left corner of the badge.

6.3.1.2 The State of Maine seal is in the upper right corner of the badge on a white background.

6.3.1.3 The space directly below the State Seal is the control group identifier. The background color and lettering color for OIT is purple or blue with yellow lettering, and the control group identifier is the letters "OIT."

6.3.1.4 The space in the center of the badge immediately below the picture and agency identifier is the access control area. Employee badges will have the words "Department of Administrative and Financial Services" in this space. Contractors and *Interns* will have a green bar with the word "Contractor" or "Intern" in red letters at the bottom of this space.

6.3.1.5 The area immediately below the access control area is for the *Card Holder* name. The lettering and background are of the base color for the agency.

6.4 Wearing and Care of Identification Badges.

6.4.1 All employees, contractors, and Visitors must always wear their identification badge while in access controlled areas.

6.4.2 Badges must be worn by means of a clip attached directly to the clothing, a neck lanyard, or similar device.

6.4.3 Badges must be worn on the front of the body in the area above the waist and nearer the midline than toward the sides.

6.4.4 Badges must not be worn so they are hidden in a pocket, worn under an article of clothing such as a sweater, jacket, tie, etc., or worn so that the picture is otherwise not visible, such as wearing the badge reversed, or under another badge.

6.4.5 Individuals must not alter their identification badge by obscuring any portion of the badge, drawing on the badge, affixing stickers to the badge, or otherwise defacing the badge in any way. Access badges which are altered will be disabled and

confiscated by Security staff.

6.5 Mandatory use of access badges at all doors.

6.5.1 Access badge holders must record their entry to any access controlled area by using their assigned access control badge. Badge holders must use their badge on every entry, regardless of whether the entry door is locked, unlocked, open, or closed.

6.5.2 Access badge holders must not use their access badge to grant another person access to any access controlled area unless they are directly escorting that person.

6.5.3 Access badge holders must not give their access badge to another person for granting that person access.

6.5.4 Employees and others must not facilitate the entry of another person to any access controlled area by holding the door open unless they are the escort for that person. Anyone authorized to enter an access controlled area will have either a valid access badge or be accompanied by their escort.

6.5.5 Access badge holders must not follow another person through an opened access control door without using their own access badge. This practice is often referred to as "drafting" or "tailgating" and is prohibited.

6.6 Requesting Access to OIT Office Complex.

6.6.1 A standard access request form must be filled out, approved, and delivered to the Building Security Administrator, in accordance with approved procedures when requesting access to OIT areas.

6.6.2 The current form and instructions are available online at Access Request Form[1].

6.6.3 Requests for new access or changes to access must be made by use of the form only. Other requests that do not require a change of access such as requests for replacement badges or new photo overlays may be made by an email request to OIT-Building-Access@maine.gov.

6.7 Lost, stolen, misplaced, and damaged Access Badges.

6.7.1 Lost, stolen, or misplaced badges must be reported to the security office as soon as the loss is discovered, so that the card may be deactivated from the access control system. Failure to notify the security office in a timely manner could result in a breach of building security using the misplaced badge.

6.7.2 The security office will produce a monthly management report detailing all cards which are replaced, the cardholder name, and the reason for replacement.

6.8 Temporary access badges issued for *Resident Employee* lost or misplaced badges.

[1] https://footprints.state.me.us/footprints/security.html

6.8.1 Resident Employees who arrive for work without their Personal Access Badge, must sign in and out at the Security Office upon entering or leaving the *Building Complex*.

6.8.2 Resident Employees will be issued a temporary access badge for the day. This temporary badge will grant access to the doors nearest the reception desk windows.

6.8.3 When a temporary badge is issued due to loss or theft, the Resident Employee's *Personal Badge* is disabled.

6.8.4 Temporary badges are issued for a 1-day period, and access for these badges will expire at 5PM of the day issued.

6.8.5 Temporary badges must be returned to the security office before leaving the building at the end of the workday.

6.9 Temporary access badges issued for *Non-Resident Employee* lost or misplaced badges.

6.9.1 Non-Resident Employees who arrive for work without their Personal Access Badge will be handled in accordance with the rules for OIT *Business Visitors*.

6.10 Contractor and Intern access.

6.10.1 Resident Contractors and Interns

6.10.1.1 Resident Contractors and Interns will be given an access badge identifying them as a Contractor or Intern.

6.10.1.2 This badge will be retained by the Resident Contractor or Intern and handled as an employee badge.

6.10.1.3 Temporary Resident Contractor or Intern access badges may be issued in accordance with the procedure outlined for Resident Employees under Section 6.8.

6.10.1.4 Resident Contractor or Intern badges will be the same as the basic agency layout for the agency they are Contracted or Interned to, but will have a green bar with the word "Contractor" or "Intern" in red letters at the bottom of the access control area.

6.10.2 *Non-Resident Contractors*

6.10.2.1 Non-Resident Contractors will be pre-authorized within the access control system, but will not be issued a Personal Access Badge.

6.10.2.2 Non-Resident Contractors will be required to sign-in. They will be given a temporary contractor badge, and access will be enabled for the day based on their pre-authorized access level.

6.10.2.3 Non-Resident Contractors who have not been pre-authorized in the access control system will be given an ID only badge. They must always be accompanied while in the building.

6.10.2.4 The contractor must return the access badge to Security and sign-out when leaving the building.

6.11 Building Visitors – General Policies.

6.11.1 All Visitors must enter the premises through the 1st floor main entrance only.

6.11.2 Visitors will be required to sign a log form indicating their name, whom they represent, person to be visited, date and time in and out, and form of ID presented.

6.11.3 All Visitors must present a current picture ID when signing in. The photo ID must have a validity date, photo, and signature. Acceptable IDs and form of ID are:

6.11.3.1 Passport
6.11.3.2 Valid Motor Vehicle Operator's License
6.11.3.3 State personal identification card
6.11.3.4 State of Maine photo ID access badge
6.11.3.5 Federal or other governmental ID
6.11.3.6 A company photo ID
6.11.3.7 Any other photo ID showing the face, ID expiration date, signature, and issuing agent information such as organization name

6.11.4 The Security Officer on duty will note the form of the photo ID presented in the space provided on the sign in log.

6.11.5 Visitors who are unable to present a current photo ID, or refuse to present a photo ID, must not be permitted access to high security OIT areas.

6.11.6 Visitors must sign out when leaving the building.

6.11.7 Temporary ID badges will be issued to Visitors who will be visiting access control areas. Temporary ID badges are not required for Visitors to non-access control areas.

6.11.8 Temporary badges must be turned in to the security office when signing out.

6.11.9 It is not necessary to sign out if leaving the building temporarily to have a smoke break, take a brief walk, get something out of the car, etc.

6.11.10 It is necessary to sign out if leaving the building complex for an extended period such as attending a meeting at another location, going out for lunch, etc.

6.11.11 Employees who admit Visitors to the building without ensuring they are properly signed in will be deemed in violation of this *Access Policy*.

6.12 OIT Business Visitors

6.12.1 OIT Business Visitors who present a valid photo ID, and have a scheduled appointment with an OIT employee, will be given a badge indicating "OIT Visitor" These Visitors must however still be accompanied while in *OIT High Security Areas*. The badge color is red.

6.12.2 OIT Business Visitors who do not have a scheduled appointment with an OIT employee, who have an appointment with a contractor only, must not be permitted access to any high security OIT area regardless of identification presented, and must always be accompanied while in other parts of the building. Such Visitors will be

given a badge indicating "OIT Visitor – must be escorted." The badge is red with black lettering on it.

6.12.3 OIT Business Visitors who are unable to present a current photo ID or refuse to present a photo ID, must not be permitted access to OIT High Security Areas, and must always be accompanied while in the building. These Visitors will be given a badge indicating "OIT Visitor – must be escorted." The badge is red with black lettering on it.

6.12.4 The Security Officer on duty will call the person to be visited. If the person to be visited is not available, the Security Officer on duty will contact the OIT administrative staff to let them know the Visitor has arrived. OIT staff will find the person to be visited, find an alternate, or escort the Visitor themselves.

6.12.5 OIT business visitors may not visit Maine Revenue Service (MRS) areas unless escorted by someone authorized to be in those areas.

6.12.6 Visitors must sign out and return the temporary badge to the security office upon leaving the building.

6.13 OIT *Personal Visitors*

6.13.1 OIT Personal Visitors such as family, friends, etc. must sign in with the Security Officer.

6.13.2 Personal Visitors will be issued "OIT Visitor" badges regardless of ID presented.

6.13.3 All Personal Visitors must always be supervised while in the OIT office area.

6.13.4 Personal Visitors are not allowed access to Maine Revenue Service (MRS) areas at any time.

6.13.5 Personal Visitors must sign out and return the temporary badge upon leaving the building.

6.14 Card Holder termination procedures

6.14.1 Supervisors must collect the access badge from any terminating employee under their supervision, and return it to the security office for destruction.

6.14.2 Supervisors must, at a minimum, notify the security office of employee termination immediately upon termination, or of the expected date and time of termination whether the access badge is collected or not.

6.14.3 Supervisors must notify the security office to disable access for an employee expected to be out for an extended period such as maternity leave, extended illness, sabbatical, or any other extended period when the employee is not expected to report for work.

6.14.4 Contract and Intern administrators must collect access badges from all contracted or Intern employees when they have finished their work.

6.14.5 Contract and Intern administrators must collect access badges from contracted or Intern employees if they leave the contracted project, even if they are expected to return at a future date.

6.14.6 Contract and Intern administrators must immediately inform security if a contracted employee or Intern is leaving for any reason including a scheduled vacation or other interruption of work where the Contractor or Intern is not expected for some period of time.

6.14.7 Employees and Contractors or Interns are not permitted to retain any access badge, access badge overlay, or other form of photo identification issued under this Policy after termination.

6.15 Use of emergency exits restricted to emergency events only.

6.15.1 Employees must not use emergency exits except:
6.15.1.1 During an actual event when emergency alarms are activated.
6.15.1.2 During a fire or evacuation drill when emergency alarms are activated.

6.15.2 Security personnel and building management personnel may use the emergency exits in the performance of their assigned job duties such as performing periodic checks to ensure the door will open, and to see that the door is locked.

6.16 Policy violations.

6.16.1 Any employee who notes a violation of this Policy must report the violation to the security officer on duty or appropriate management level personnel as soon as possible.

6.16.2 Security will record information regarding the violation and forward the report to the appropriate management personnel.

6.16.3 Management will contact the violator and apply disciplinary action as appropriate.

6.17 Special Events

6.17.1 Persons attending special events open to the public may be subject to discretionary rules administered by the Security Manager.

6.17.2 The Security Manager must approve each event as qualifying under this section. Examples of special events are Blood Drives, Employee Recognition events, and Retirement parties.

6.17.3 The Security Manager may, at his discretion, suspend any or all of the following rules for event participants during these events:
6.17.3.1 Visitor sign in
6.17.3.2 Photo ID

6.17.3.3 Visitor badge

7.0 Document Information

Initial Issue Date: November 18, 2009
Latest Revision Date: April 4, 2019 – To update Document Information.

Point of Contact: Security Compliance and Policy Manager, OIT.Policy-Compliance@Maine.Gov
Approved By: Chief Information Officer, OIT

Legal Citation: Title 5, Chapter 163: Office of Information Technology[2].
Waiver Process: See the Waiver Policy[3].

[2] http://legislature.maine.gov/statutes/5/title5ch163sec0.html
[3] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/waiver.pdf