



Policy Owner:	VP of Operations
Original Issue Date:	11/16/15
Revision Number:	2
Revised Effective Date:	11/17/20
Approved By:	Policy & Ethics Committee

PHYSICAL ACCESS CONTROL POLICY

PURPOSE

ATC Management Inc. ('ATC' or the 'Company') recognizes that in order to fulfill its job responsibilities, all employees, contingent workers, and those employed by others to perform work on ATC premises or who have been granted unescorted physical access to ATC facilities require use of ATC-provided ID badges, PIN code, and/or keys. This policy outlines the acceptable use of these resources.

SCOPE

This policy applies to all ATC employees and Contingent Workers who have been granted unescorted physical access to one or more ATC facilities.

DEFINITIONS

Access Steward – Designated by the ATC functional managers to authorize requests for controlled access.

ATC Facilities – A space and/or a building owned or controlled by ATC via a lease and/or other arrangement.

Contingent Worker – See [Worker Classification Policy](#)

Point of Contact – The primary liaison at the vendor providing Contingent Worker services at ATC.

RESPONSIBILITIES

Employees and Contingent Workers are responsible for:

- Successful completion of a Personnel Risk Assessment prior to gaining unescorted physical access to ATC in accordance the [Personnel Risk Assessment Policy](#)
- Completing Security Awareness Training prior to gaining unescorted physical access to ATC, and annually thereafter
- Prominently displaying their identification badge at or above the hipline at all times within an ATC office or substation
- Presenting ATC issued badge to the card reader to enter reader-controlled areas
- Presenting ATC issued badge to the reader and entering their Personnel Identification Number (PIN) to gain entry to areas that are subject to NERC Critical Infrastructure Protection (CIP) Standards
- Returning ATC issued badge and/or keys to ATC upon termination of employment or completion of assignment with ATC

- Escorting visitors that do not have unescorted physical access privileges to ATC, at both ATC offices and substations
 - Note: A visitor badge must be issued and physically worn by guests at all times while within ATC offices.
- Keeping visitor(s) within eyesight at all times
- Actions of their visitor(s) while performing escorting duties
- Reporting missing, damaged, or malfunctioning access control devices
- Immediately reporting lost, stolen, or damaged badges and/or keys to ATC Corporate Security
- Responding to inquiries regarding possession of substation keys (as applicable)
- Immediately self-correcting and self-reporting access errors to ATC Corporate Security

Supervisors are responsible for:

- Requesting and/or approving appropriate physical access for subordinates, including Contingent Workers
- Providing appropriate business justification for access when applicable
- Notifying the Point of Contact upon Contingent Worker termination
- Collecting ATC property, to include access credentials and keys, upon termination

Human Capital is responsible for:

- Completing Personnel Risk Assessments, in accordance with the [Personnel Risk Assessment Policy](#)
- Collecting ATC property, inclusive of access credentials and keys, upon employee termination

Point of Contact is responsible for:

- Coordinating background screens for Contingent Workers, in accordance with the [Personnel Risk Assessment Policy](#)
- Notifying ATC’s Human Resources department if a Contingent Worker is no longer employed by the company
- Collecting ATC property, to include access credentials and keys, upon termination or when Contingent Worker is identified as no longer performing a role for ATC

Access Steward is responsible for:

- Approving access privileges to areas where required

Corporate Security is responsible for:

- Issuing access credentials when applicable
- Issuing substation keys when applicable
- Disabling electronic access credentials (i.e. ID badge and PIN) upon notification of termination or other notification that physical access is no longer required
- Monitoring controlled access points
- Responding to alarms generated at controlled access points

Inappropriate Use of Access Controls

- Allowing an unauthorized person (e.g. no ATC ID or ATC visitor badge) to follow you into ATC offices
- Allowing another individual to use your ID badge and/or PIN for access or identification purposes
- Allowing another individual to use your key for access purposes
- Passing on key(s) to your replacement or successor
- Sharing your PIN with anyone
 - Note: Use of authorized encrypted password vaults is permitted for the storage and retrieval of PINs.
- Tampering with or disabling access control devices
- Leaving an opened controlled access point unattended

REPORTING

It is the responsibility of all ATC employees and Contingent Workers to report any suspected violations of this policy in accordance with ATC's [Open Door Policy](#).

EXCEPTIONS/VIOLATIONS

All escorts must keep visitors within eyesight at all times, except within restrooms.

The use of an ATC visitor badge at ATC substations is not required; all visitors must sign in and out on the visitor log.

Exceptions to this policy require the approval of the Policy Owner listed above.

Employees who violate this policy are subject to disciplinary action up to and including termination.