



## PHYSICAL ACCESS CONTROL POLICY

Effective Date: 05/01/2026

---

### 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, or may be granted unescorted physical access to ATC facilities require use of ATC-provided ID badges, PIN codes, 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.

**Visitor** – Any individual that is not authorized for unescorted physical access to secure areas within ATC facilities. This includes ATC Employees and Contingent Workers who are not authorized for access to areas subject to NERC Critical Infrastructure Protection (CIP) Standards and Substations with Enhanced Security (SES).

### 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 ATC issued identification badge at or above the hipline at all times within an ATC office or substation
- Removing or concealing their ATC issued identification badge when not inside an ATC office or substation
- Presenting ATC issued identification badge to the card reader to enter reader-controlled areas
- Presenting ATC issued identification 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
- Ensuring that reader-controlled/reader and PIN doors close securely behind them once they pass.
- Returning ATC issued identification badge and/or keys to ATC upon termination of employment or completion of assignment with ATC

- Registering visitor to ATC offices in advance of the expected visit.
- Escorting visitors that do not have unescorted physical access privileges to ATC, at both ATC offices and substations
  - Note: An ATC visitor identification badge must be issued and physically worn by guests at all times while within ATC offices.
- Keeping visitor(s) within eyesight at all times
- The 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

**Point of Contact is responsible for:**

- Coordinating background screens for Contingent Workers, in accordance with the Personnel Risk Assessment Policy
- Notifying ATC 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

**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

**NON-RETALIATION**

ATC strictly prohibits retaliation in any way against anyone who has honestly made a report or complaint, expressed a concern about inappropriate conduct or cooperated in an investigation. Disciplining or otherwise disadvantaging an individual because they in good faith reported a potential concern or cooperated in an investigation is, itself, a violation of ATC 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.