Document No.:	BP-1601				
Title:	Physical and Cyber Security Business Practice				
Department:	External Affairs				
Previous Date:	07-02-2020	Issue Date:	11-28-2023	Revision:	V3
Sharing Limits:	*Any hard copy reproductions of this Business Practice should be verified against the on-line system for current revisions.*				

Table of Contents

1 PURPOSE

This Business Practice outlines the physical and cyber security measures that are implemented between ATC and its interconnected entities (IEs). The physical security systems installed at joint-use substations are coordinated installations between ATC and its IEs. Cyber security measures are in place to allow safe and secure access to ATC's Cyber Assets or Systems used to operate and maintain the electric transmission system.

1.1 SCOPE AND APPLICABILITY

This Business Practice includes aspects of physical and cyber security as it relates to the systems in place that affect both ATC and its IEs. Other physical and cyber security systems used solely for ATC or its IEs are not covered here.

ATC continuously evaluates risk and makes changes to measures as appropriate.

1.2 PHYSICAL SECURITY AND CYBER SECURITY

The cyber/information security functions use the NIST Cyber Security Framework (NIST CSF) as a control framework.

> *The Framework is voluntary guidance based on existing standards, guidelines, and practices for critical infrastructure organizations to better manage and reduce cybersecurity risk. In addition to helping organizations manage and reduce risks, the NIST CSF was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders.*

The physical security function references the ASIS Protection of Assets (PoA) framework to identify and implement a variety of protections based on internal and external threat factors.

Applicable laws and regulations to which Security controls are applied, include but are not limited to:

- FERC Order 693
- FERC Order 706 (NERC CIP)
- Strengthening American Cybersecurity Act

Additional risk assessments are performed on an individual site bases which includes threats, vulnerabilities, and other consequences. Installation and mitigation measures may be adjusted based on risk assessment results.

2 ROLES AND RESPONSIBILITIES

Regional Manager Customer Engagement

- Schedules and facilitates meetings between ATC and IE
- Provides issue resolution management
- Maintains key points of contact for physical and cyber security
- May serve as ATC Sponsor to establish access to ATC sites and systems

ATC Sponsor of the Contingent Worker (CW)

- Ownership of primary business relationship for the CW
- Initiates position/contract request in ATC Human Capital Management (HCM) system
    - Identifies access prerequisite needs via Job Profile selection
- Submits and approves access/provisioning requests in ATC's Identity Access Management (IAM) system

- Provides justification for access needs
- Communicates/initiates Contingent Worker terminations to HR in event of employment status or access requirement change

ATC CW Admin (performs administrative tasks on behalf of ATC Sponsors)

- Initiates position/contract request in ATC Human Capital Management (HCM) system
  - Identifies access prerequisite needs via Job Profile selection
- Submits access/provisioning requests in ATC's Identity Access Management (IAM) system
  - Provides justification for access needs

ATC Contingent Worker Program Manager (CWPM)

- Processes contract/position requests
- Manages communication/outreach to Contingent Worker and identifies Points of Contact throughout onboarding process, including relevant ATC policies and procedures
- Monitors prerequisite completion to ensure adherence to Contingent Worker Program
- Process and communicate Contingent Worker terminations to ATC stakeholders

ATC Contingent Worker

- Completes applicable prerequisites (screenings, forms, training, etc.)
- Complies with all applicable ATC policies and procedures

Point of Contact (POC)

- Works with ATC Sponsor to provide/contract CW resources
- Ensures CW candidates are completing required onboarding activities
- Acknowledges and confirms CW employment verifications
- Contacts ATC Immediately in event of CW termination of service
- Ensures collection and return of applicable ATC credentials if/when no longer needed (badges, keys, computer equipment, etc.)

Visitor/Worker to ATC Sites

- Completes prerequisites prior to access
- Ensures access needs are requested and approved
- Completes weekly verification of employment status and access need (CIP)

3 EXPECTATIONS FOR ACCESS TO ATC SYSTEMS AND SITES

3.1 ACQUIRING ACCESS TO ATC SITES AND SYSTEMS

Requests for access to ATC sites and systems are managed through ATC's Contingent Worker Program. This process is initiated by contacting the ATC Sponsor. To receive information regarding access to ATC sites, contact the ATC Customer Engagement Regional Manager.

At existing sites where security upgrades impact current access procedures, the Customer Engagement Regional Manager works with the affected IE to begin coordination with the Contingent Worker Program Manager to ensure IE maintains access to necessary assets.

When connecting to ATC Cyber Assets or Systems, IEs are expected to use secure methods and operate in accordance with:

- ATC's NERC CIP Cyber Security Policy and Appropriate Use of ATC Resources Policy
- Practices defined in ATC's annual Security Awareness Training
- Onsite signage, instructional documentation, and provided hardware if any
- Practices defined within legal contracts between ATC and the IE

3.2 MAINTAINING ACCESS TO ATC SITES AND SYSTEMS

To maintain access to ATC Sites and Systems, an ATC Contingent Worker must complete the following actions:

- Complete required training as assigned through ATC's Contingent Worker Program
- Comply with ATC policies and procedures
- Provide notification of changes to employment status and access needs

3.3 DEACTIVATING ACCESS TO ATC SITES AND SYSTEMS

Contingent Worker deactivations and terminations are to be communicated to HR by:

- Designated Point(s) Of Contact (POC's)
  - Termination of Service (TOS) process/form submitted to ATC
- ATC Sponsor
  - Termination initiation in ATC Human Capital Management (HCM) system
  - Phone call to ATC Corporate Security hotline (after hours)

4 PROCESS FOR IMPLEMENTATION OF OR MODIFICATIONS TO SECURITY MEASURES AT A NEW OR EXISTING FACILITY

4.1 CRITERIA

Following asset identification and the physical security risk assessment, the effectiveness of existing security and operational practices is evaluated. Based on this evaluation, recommended actions and mitigation measures are developed that will cost effectively mitigate risks by identifying threats and reducing vulnerabilities and/or consequences for ATC and the IE. Actions may include changes to ATC and IE operational programs, policies or procedures. ATC will then develop a plan to install additional security mitigation measures as required to effectively reduce operational risk.

4.2 INITIATION OF SECURITY MEASURES BY ATC

Following an ATC site survey and risk assessment results, ATC determines an appropriate physical security package through the project development process. Discussion and collaboration with all asset owners at the site to review proposed security measures occurs following development of a preliminary project scope and schedule, adhering to the ATC project request process. At an IE-controlled site, ATC will initiate consultation with IE to discuss proposed security measures to ensure consensus on appropriate protection. The Customer Relations Regional Manager communicates available project information with impacted IE.

The final design of implemented measures is determined during detailed design with input from ATC Corporate Security, ATC Asset Management and IE.

4.2.1 Cyber Security

ATC is responsible for notification of cyber security changes to the IE personnel.

4.3 INITIATION OF SECURITY MEASURES BY INTERCONNECTED ENTITY

At an IE-controlled site, ATC requests consultation with IE to discuss proposed security measures to ensure appropriate protection is in place. IE can contact the Customer Engagement Regional Manager with a proposal.

5 COST RESPONSIBILITY

5.1 PHYSICAL SECURITY

Cost allocation for physical security measures implemented at a joint-use substation is documented in Joint Use Substations – Cost Responsibility for Common Facilities Business Practice. This Business Practice is available at:

http://www.atcllc.com/customer-relations/business-practices/

5.2 CYBER SECURITY

IEs are not billed for ATC-initiated work for implementation of cyber security measures at a joint-use substation.

6 COMPLIANCE

Each entity is responsible for their compliance obligations. When implementing physical security measures at Joint-Use Substations, ATC will coordinate with the impacted IE.

Information shared and exchanged through the processes described in this Business Practice may be Critical Energy Infrastructure Information (CEII) and subject to ATC's Identification and Protection of CEII Materials Procedure.

7 DOCUMENT REVIEW

This document will be reviewed annually.

8 RECORDS RETENTION

Documents are maintained per the Records Retention Schedule.

Records Management Index System (RMIS)

Records Management Policy #2002-2 Revision Information

Rev.	Date	Author	Description
1.0	09-16-2016	Ben Stuart	Original
2.0	07-02-2020	Matt Waldron	Transient Cyber Assets appended to Expectations
3.0	11-18-2023	Marcia Louden	Updated template, branding, adjusted policies with renaming conventions, and aligned cyber, physical and information security descriptions with Enterprise Security program language

Approved by:	Date:
Trevor Stiles TD Stiles	11/28/2023