Policy Owners:	Executive Vice President, CFO & Treasurer
Original Issue Date:	10/10/00
Revision Number:	10
Revised Effective Date:	1/1/23
Approved By:	Policy & Ethics Committee

ACCEPTABLE USE OF ATC RESOURCES POLICY

PURPOSE

The purpose of this policy is to set expectations regarding ATC Management Inc. ('ATC' or the 'Company') Electronic Resources and ATC Information provided to users to conduct business operations.

SCOPE

This policy applies to all users of ATC Electronic Resources including employees, contractors, contingent workers and third parties performing work on ATC's behalf (collectively referred to as 'Users').

DEFINITIONS

ATC Information – Data or documents that are used to support ATC business activities.

Electronic Resources – Internet, electronic mail, telecommunications, hardware, software and applications used to conduct ATC business (inclusive of externally hosted environments and personal devices containing ATC information).

Hardware Device – Media that includes, but is not limited to, the following examples:

- Laptop/notebook/tablet computers
- Smartphones and other mobile/cellular phones
- Ultra-mobile computers and wearables (e.g. smartwatch)
- Portable media devices (e.g., USB thumb and external hard drives)
- Any personal devices capable of storing corporate data and connecting to a network
- Servers
- Telecommunication infrastructure
- Appliances
- Substation Technologies

Information Technology functions – Departments or teams assigned responsibility for the governance or administration of ATC systems or electronic resources. Including, but not limited to:

- Information Technology department
- Corporate Security team
- Energy Management Systems team
- Metering & Control team
- System Protection team

Software – Program designed to fulfill a particular purpose (e.g., cloud products, email services, file shares).

System – Self-contained interoperating objects (interconnected Applications/Software/Firmware, Interface, Storage/Database, Hardware, appliances)

RESPONSIBILITIES

Users are responsible for:

- Using ATC electronic resources primarily for business purposes[1]
- Physically securing and safeguarding ATC-owned Systems and personal devices used to access ATC Information
- Managing and securing ATC account credentials
- Locking device screens when unattended
- Securing personal devices accessing ATC information with passwords or biometric control (a PIN is not sufficient)
- Monitoring others' use of their devices to ensure sensitive data is secure[2]
- Using ATC-provided access methods (e.g., VPN, Connect, Cloud Desktop) to connect personal devices used for Company business
- Obtaining Enterprise Technology Director/VP-level approval for the use of shared accounts
- Notifying the IT Service Desk of foreign travel if electronic resources are needed (electronic resources may not be permitted in certain locations)
- Promptly reporting a lost or stolen device to the IT Service Desk
- Installing and updating personal devices with anti-virus/anti-malware software
- Providing non-ATC removeable media devices to the IT Service Desk for scanning of malware prior to use
- Physically securing and encrypting all ATC information stored on a removeable media device

Users are prohibited from:

- Sharing or disclosing security technology assets (e.g., security token, PIN, badge) or account credentials (e.g., user name, password) with others
- Using ATC credentials for personal purposes
- Using the same credentials for personal and ATC accounts
- Using personal email for company business
- Using company email for personal business
- Forwarding (including auto-forwarding) ATC information to personal email accounts
- Storing ATC passwords on personal devices
- Storing personal/private information on ATC electronic resources
- Connecting a personal or non-ATC owned devices to any physical, wired network connection other than in the office zero-zone area
- Connecting a personal or non-ATC computer accessory, storage device, or other peripheral to any ATC owned computer devices with the exception of headset, mouse, keyboard, camera, monitor, or other peripheral exception approved by the Enterprise Technology Director/VP
- Connecting a personal or non-ATC owned device to the "corpaccess" WiFi network or any other ATC network not designated for non-ATC devices
- Establishing or attempting to establish a wired or wireless (Bluetooth, near-field, Wi-Fi, etc.) network that is attached in any manner to an ATC network

[1] Limited personal use of electronic resources is permissible if it doesn't negatively impact user productivity, cause additional Company expenses or compromise ATC in any way.
[2] The device owner is ultimately responsible for any actions performed on their device/account.

- Using ATC-owned devices for unlawful or inappropriate purposes (e.g. copyright infringement, personal gain/solicitation, spreading malware, accessing objectionable[3] content)
- Altering, circumventing or removing security-related applications and configurations from ATC-owned devices (unless otherwise directed by IT Security)
- Recording or transcribing meetings or conversations, except where authorized by management for legitimate business purposes[4]
- Using third-party file sharing services for ATC confidential information assets

Information Technology functions are responsible for:

- Granting user access to electronic resources, as appropriate
- Approving all hardware, software, licenses and/or service agreements that include ATC information sharing, storage and protection (both ATC and non-ATC assets) – in accordance with the Legal Review, Procurement and Expenditures Authorization Policy
- Documenting authorization of any shared accounts
- Using elevated or administrative rights for necessary job functions only
- Promptly performing a remote wipe of lost or stolen devices
- Scanning non-ATC removeable media devices for potential malware
- Applying security protections (e.g. system hardening, multi-factor authentication (MFA)) to ATC systems, commensurate with risk and/or standardized expectations

ATC reserves the right to:

- Restrict connectivity of non-ATC assets to ATC electronic resources
- Control data transfer to/from non-ATC devices
- Monitor and review all activity on ATC electronic resources
- Access ATC information stored on ATC-owned and personal devices[5]
- Place litigation holds on electronically stored information on ATC-owned or personal devices used to access ATC electronic resources (this may include personal data if mixed in with business data)

REPORTING

It is the responsibility of all users to report any suspected violations of this policy, in accordance with ATC's Open Door Policy.

EXCEPTIONS/VIOLATIONS

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

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

This policy is not intended to restrict or interfere with any employee's federal or state labor law rights, including all rights under the National Labor Relations Act.

---

[3] Objectional content that may be viewed as maliciously false, obscene, physically threatening, disparaging or unlawful harassment / bullying.

[4] Recording or transcribing is prohibited to protect the confidentiality of the Company's trade secrets and confidential business information (including, but not limited to, processes, techniques, systems, and strategies) and the freedom of Users to communicate without concern of being recorded without their consent, Examples of legitimate business purposes include company-wide meetings and training sessions. Under no circumstances should meetings or conversations be recorded without the awareness and consent of all parties involved.

[5] ATC assumes no liability for personal or non-ATC information stored on ATC electronic devices.