ACCEPTABLE USE OF ATC RESOURCES POLICY

Effective Date: 10/15/2024

PURPOSE

The purpose of this Policy is to set expectations regarding ATC's Electronic Resources and ATC Information provided to employees, contractors, contingent workers and third parties for the purpose of conducting ATC's 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'). All users must use ATC's Electronic Resources responsibly and in compliance with company policies.

DEFINITIONS

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

Electronic Resources – Internet, electronic mail, telecommunications, Hardware, Software, messaging applications, and other applications used to conduct ATC business (inclusive of externally hosted environments and personal devices containing ATC Information).

Hardware Media Devices – Media that includes, but is not limited to:

- 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 an ATC network
- Servers
- Telecommunication infrastructure
- Appliances
- Substation Technologies

Messaging Applications - Applications used for mobile-to-mobile transmission of multimedia messages, including encrypted and ephemeral messaging applications.

Objectionable Content – content that may be viewed as maliciously false, obscene, physically threatening, disparaging or unlawful harassment / bullying.

Technology Onboarding – Activities relating to the introduction, proposals, contract discussion, acquisition, and use of new technology or services, including non-committal activities such as pilot or proof-of-concept testing, demo / evaluation use of Hardware or Software, accessing external services for processing or storage of ATC Information, permission to expanded features of existing Software, etc.

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] and not avoiding, circumventing, or bypassing security controls or corporate policies
- 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
- Not copying ATC information onto personal devices that do not adhere to ATC security requirements
- Monitoring others' use of their devices so that sensitive data is secure[2]
- Using ATC-provided access methods (e.g., VPN, Connect, Cloud Desktop) to connect personal devices used for ATC business
- Obtaining appropriate approval for the use of shared accounts
- Notifying the Service Desk of foreign travel if Electronic Resources are needed (i.e., Electronic Resources may not be permitted in certain locations)
- Promptly reporting a lost or stolen device to the Service Desk
- Installing and updating personal devices with anti-virus/anti-malware software
- Providing non-ATC removeable Hardware to the Service Desk for scanning of malware, and using only secured and encrypted removable Hardware for use with ATC Information
- Reporting any suspicious activities
- Abiding by litigation holds on electronically stored information on ATC-owned or personal devices used to access ATC Electronic Resources
- Preserving and respecting the confidentiality of ATC information, work products and practices at all times (including during the use of Artificial Intelligence (AI) systems) by using authorized tools, techniques and procedures to manage the information
- Accessing only approved external Artificial Intelligence (AI), Machine Learning (ML) or Deep Learning (DL) systems
- Verifying the output of products (including Artificial Intelligence (AI)) to ensure the output does not lead to fraudulent, destructive, or inappropriate system usage; poor, biased, and/or unethical practices or decisions; reputational and/or financial harm to ATC
- Maintaining control and responsibility in the use of information, tools, technologies, and services (including AI) and its outcomes
- Citing the sources of all generated or processed information (including AI/ML) contained in official documents, presentations, or materials used for strategic planning or decision-making

[1] Limited personal use of electronic resources is permissible if it does not 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.

Users are Prohibited from:

- Sharing or disclosing security technology assets (e.g., security token, PIN, badge) or account credentials (e.g., username, password) with others
- Technology Onboarding or procuring Hardware, Software, licenses and/or services, or modifications to associated agreements or functionality (that include ATC Information sharing, storage, and protection) without appropriate involvement
- 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
- Using personal Messaging Applications for conducting ATC 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 ports (utilize Wi-Fi only)
- Connecting a personal or non-ATC computer accessory, storage device, or other peripheral to any ATC owned computer devices apart from headset, mouse, keyboard, camera, monitor, or other peripheral exception registered with and approved by the Service Desk
- Connecting a personal or non-ATC owned device to the “CorpAccess” Wi-Fi 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
- Using ATC-owned devices for unlawful or inappropriate purposes (e.g., copyright infringement, personal gain/solicitation, spreading malware, accessing Objectionable Content)
- Altering, circumventing, or removing security-related applications and configurations from ATC-owned devices
- Recording meetings or conversations, except where authorized by management for legitimate business purposes [3]
- Using third-party file sharing services for ATC confidential information assets
- Publishing or uploading ATC proprietary or confidential information (or protected private partner organizations) to public-facing or non-approved AI (artificial intelligence) or Machine Learning (ML) tools
- Communicating about ATC’s business or sharing ATC Information on any messaging applications or other communication platforms that are not approved by ATC (following the External Communications Policy)

[3] Recording 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.

Subject to applicable law, ATC Reserves the right to:

- Restrict connectivity of non-ATC assets to ATC Electronic Resources
- Control transfer of ATC Information to/from non-ATC devices
- Monitor and review all activity on ATC Electronic Resources, including data contained within messaging platforms)
- Access ATC information stored on ATC-owned and personal devices [4]
- 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 ATC employees to report any suspected violations of this Policy, in accordance with ATC's Open Door Policy.

NON-RETALIATION

ATC 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

Exceptions to this Policy require the approval of the Policy Owners listed above. Employees, contingent workers or contractors who violate this policy are subject to disciplinary action, up to and including termination.

This Policy is not intended by ATC, and will not be interpreted or applied by ATC, to prohibit or dissuade employees from engaging in legally protected activities such as discussing wages, benefits or terms and conditions of employment.

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