ACCEPTABLE USE OF ATC RESOURCES POLICY

Effective Date: 08/01/2026

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

- **Artificial Intelligence (AI**): Systems that simulate human capabilities such as perception, reasoning, learning, and decision-making.
- **Business Record:** An official record of a business-related act, condition, or event. This includes things like meeting minutes, contracts, and documents with retention requirements.
- **Company Business:** Any activity that contributes to ATC's goals, operations, or revenue.
- **Deep Learning (DL):** A subset of ML using neural networks to model complex patterns.
- **Electronic Resources:** This is a broad term covering everything from the internet, email, and telecommunications to hardware, software, messaging apps, and social media platforms used for ATC business. It also includes personal devices that contain ATC information.
- **Hardware Media Devices:** Physical devices like laptops, smartphones, tablets, external hard drives, and even wearables that can store company data or connect to an ATC network.
- **Enterprise Technology Functions:** The teams responsible for managing ATC's systems and electronic resources, such as the Systems and Security Integration division, Audit, Risk Management, and Compliance, and others.
- **Machine Learning (ML):** A subset of AI that learns from data to improve performance.
- **Messaging Applications:** Apps used for sending multimedia messages between mobile devices, including encrypted and ephemeral (momentary) ones.
- **Objectionable Content:** Content that is maliciously false, obscene, physically threatening, disparaging, or constitutes unlawful harassment or bullying.
- **Peripherals:** External devices that connect to a computer to enhance its functionality, like keyboards, mice, monitors, and printers.
- **Public AI Tools:** Any AI system not operated within ATC's private tenant.
- **Technology Onboarding:** The process of introducing, acquiring, and using new technology or services, including pilot testing and accessing external services for ATC information.
- **Software:** Programs designed for a specific purpose, such as cloud products, email services, or file shares.
- **System:** Interconnected applications, software, firmware, hardware, and storage that work together.
- **Users:** This includes all employees, contractors, contingent workers, and third parties who use ATC Electronic Resources or perform work on ATC's behalf.

RESPONSIBILITIES

Users are responsible for:

- **Prioritizing Business Use:** Using ATC Electronic Resources primarily for business purposes. Limited personal use is allowed if it doesn't negatively impact user productivity, cause additional corporate expenses, or put ATC at risk. The use of ATC issued electronic resources for personal business affairs is not permissible (e.g., filing personal taxes, using ATC email for other businesses or personal hobbies).
- **Securing Devices:** Physically securing ATC-owned devices and your personal devices used for ATC information.
- **Protecting Credentials:** Managing and securing your ATC account credentials.
- **Locking Screens:** Locking your device screen when you step away.
- **Monitoring Personal Devices:** Monitoring how others use your personal devices to ensure sensitive data remains secure. You are ultimately responsible for any actions taken on your device or account.
- **Using Approved Access Methods:** Using ATC-provided methods (like VPN, Connect, or Cloud Desktop) to connect personal devices used for ATC business.
- **Shared Accounts:** Getting approval from a System and Security Integration (SSI) Director/VP for using shared accounts.
- **Foreign Travel Notification:** Notifying the Service Desk if you plan foreign travel and need electronic resources, as they may not be permitted in all locations.
- **Reporting Lost/Stolen Devices:** Promptly reporting a lost or stolen device to the Service Desk or the Cyber Security hotline after business hours.
- **Antivirus Software:** Installing and updating antivirus/anti-malware software on personal devices used for ATC business.
- **Scanning Removable Hardware:** Providing non-ATC removable hardware to the Service Desk for malware scanning and using only secured and encrypted removable hardware with ATC Information when possible.
- **Reporting Suspicious Activity:** Reporting any suspicious activities to the Service Desk and/or Security teams.
- **Recording/Transcription Services:** Verifying third-party recording/transcription service safeguards and consulting Enterprise Technology functions before account registration to prevent potential data exposure.

Users are Prohibited from:

- **Sharing Security Assets:** Sharing security technology assets (e.g., security tokens, PINs, badges) or account credentials (e.g., usernames, passwords) with others.
- **Unauthorized Technology Onboarding:** Onboarding or purchasing hardware, software, licenses, or services, or modifying associated agreements or functionality that involves ATC Information sharing, storage, and protection without involving an Information Technology Business Partner and following the Legal Review, Procurement, and Expenditures Authorization Policy.
- **Using ATC Credentials for Personal Use:** Using ATC credentials for personal purposes or using the same credentials for personal and ATC accounts.
- **Using Personal/Company Email Inappropriately:** Using personal email for company business or company email for personal business.
- **Forwarding ATC Information to Personal Accounts:** Forwarding (including auto-forwarding) ATC information to personal (non-ATC) email accounts.
- **Storing ATC Passwords on Personal Devices:** Storing ATC passwords on personal devices.

- **Storing Personal Information on ATC Resources:** Storing personal/private information on ATC electronic resources.
- **Unauthorized Device Connections:**
  - Connecting personal or non-ATC owned devices to any physical ports (use Wi-Fi only).
  - Connecting a personal or non-ATC storage device or a peripheral device that requires software or firmware to operate to any ATC-owned computer device that is not registered with and approved by the Service Desk (with the exception of charging only on corporate endpoints).
  - 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 network (Bluetooth, near-field, Wi-Fi, etc.) that is attached in any manner to an ATC network.
- **Unlawful/Inappropriate Use of ATC Devices:** Using ATC-owned devices for unlawful or inappropriate purposes (e.g., copyright infringement, personal gain/solicitation, spreading malware, accessing Objectionable Content).
- **Altering Security:** Altering, circumventing, or removing security-related applications and configurations from ATC-owned devices (unless directed by Enterprise Security Operations & Engineering).
- **Recording Without Consent:** Recording meetings or conversations for legitimate business purposes without the awareness or consent of participants. This includes confidential information like trade secrets. Unconsented recording is a violation of privacy. **Transcription services are generally approved as they enhance accessibility and record key decisions, but consent is still important for meeting recordings.*
- **Using Personal or Ephemeral (Momentary) Messaging Apps for Business** Using personal or ephemeral messaging applications for business, as these bypass record capture and introduce substantial organizational risks, such as those related to regulatory compliance, reputational damage, and legal liability.

Use of AI for Business Purposes:

- Any onboarding or use of external AI, ML, or DL systems for ATC business purposes must be approved by the Systems and Security Integration (SSI) division.
- Employees must use ATC-managed AI solutions (e.g., Microsoft Copilot) when handling any ATC business information.
- Contractors, contingent workers and third parties that use AI tools are responsible for conformance with NDAs and protecting ATC information with their use of solutions. Public or insecure AI solutions cannot be used for ATC business information.
- Humans must always maintain control and responsibility for outcomes generated by AI; employees are responsible for
  - Protecting the confidentiality, integrity, and privacy of ATC and partner information
  - Understanding bias and striving for fairness
  - Being aware of data flows and maintaining confidentiality
  - Ensuring AI output is factually correct, non-misleading, and appropriate for business use
  - Citing sources when AI-generated content is used in official documents or presentations
- AI-generated content is not considered Intellectual Property (IP) or copyrightable in the U.S. if created solely by AI, as it lacks human authorship. However, substantial human editing, curation, or creative modification of AI output can allow for copyright protection over those specific human-added elements.
- Suspected improper AI use, data exposure involving AI tools or unauthorized use of AI tools must be reported to Cybersecurity immediately.

Prohibited Use of AI

- Entering ATC confidential or proprietary information into public or non-SSI approved AI models.(Contact the Service Desk or your IT Business partner for more information).
- Using ATC AI solutions for personal activities, decision-making involving private or sensitive personal data, or personal financial/medical decisions.
- Uploading NDA-protected or partner information to public AI tools

ATC Reserves the right to:

- **Restrict Connectivity:** Restrict connectivity of non-ATC assets to ATC Electronic Resources
- **Control Information Transfer:** Control transfer of ATC Information to/from non-ATC devices
- **Monitor Activity:** Monitor and review all activity on ATC Electronic Resources, including data contained within messaging platforms)
- **Access Stored Information:** Access ATC information stored on ATC-owned and personal devices . **ATC assumes no liability for personal or non-ATC information stored on ATC electronic devices.*
- **Place Litigation Holds:** 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.