Policy Owner:	Executive Vice President, CFO & Treasurer
Original Issue Date:	10/10/00
Revision Number:	8
Revised Effective Date:	5/14/18
Approved By:	Policy & Ethics Committee

ACCEPTABLE USE OF ELECTRONIC RESOURCES POLICY

PURPOSE

ATC Management Inc. ('ATC' or the 'Company') recognizes that in order to fulfill their job responsibilities, all employees, contractors, temporary workers, and those employed by others to perform work on ATC premises or who have been granted access to ATC information/data or systems ('Users') require use of some set of ATC-provided computer based systems and services. This policy outlines the acceptable use of these resources.

SCOPE

This policy applies to all employees, contractors, temporary workers, and those employed by others to perform work on ATC premises or who have been granted access to ATC-owned computing devices, information, or systems.

This policy does not apply to systems that comprise the Energy Management System (EMS) or substation field devices.

Note: Electronic Resources included in scope for NERC CIP have additional compliance obligations, and their use must adhere to those policies and practices.

DEFINITIONS

ATC Confidential Information – Information should be classified as ATC Confidential Information when the unauthorized disclosure, alteration, or destruction of that information could expose the Company or its affiliates to a significant level of risk or negatively impact regulatory compliance, business development, or the Company's ability to continue ongoing operations. Examples of ATC Confidential Information include trade secrets and proprietary information, Critical Infrastructure Protection (CIP) Information, Critical Energy Infrastructure Information (CEII), non-public transmission function information governed by the FERC Standards of Conduct, business development information, market information relating to ATC's business practices and strategies, customers' confidential information, private employee personnel and medical records including Personal Identifiable Information (PII) and Protected Health Information (PHI), private financial information relative to the Company's operations, etc. By default, all information that is not considered public information should be treated as ATC Confidential Information. If you are unsure if information should be considered ATC Confidential Information, please check with your supervisor before disclosing the information to anyone outside of the Company. For the purposes of this policy, ATC Confidential Information does not include information regarding the workplace and work environment generally, as well as information regarding wages, compensation, or other terms and conditions of employment with ATC. Employees may disclose information about themselves, such as information related to their job performance or their job duties.

ATC Sponsor – A person that is responsible for the relationship between ATC and non-company Electronic Resources Users. This person is responsible to ensure that the Non-Company User is still active in employment with their respective organization. This person is responsible for the timely (within 24 hours) notification to Information Technology ('IT') when the Non-Company User's services are no longer required.

Authentication – Controls for providing Users the means to verify or validate a claimed identity through the presentation of something they know (*e.g*., passwords), something they own (*e.g*., hardware token), or something they are (*e.g*., fingerprint, biometrics, etc.).

CONNECT – ATC's centralized authentication portal for access to ATC's systems, both on premise and in the Cloud.

Contingent Worker – See Worker Classification Policy

Electronic Resources – Company-provided internet, electronic mail, telecommunication resources and Company-owned data, hardware, and software inclusive of externally hosted environments.

Information (Data) Custodian – An ATC employee who has management accountability for information or a set of data. The custodian is responsible for understanding who has access to the data and decides if people can be granted access to that data.

Objectionable – Anything that reasonably could be viewed as maliciously false, obscene, physically threatening or intimidating; that disparages customers, members, employees, or suppliers; or that might constitute unlawful harassment or bullying. Examples include offensive posts of statements, photographs, video, or audio meant to intentionally harm someone's reputation through malicious and knowingly false statements or posts that could contribute to a hostile work environment based on race, sex, disability, religion, or any other status protected by law or Company policy.

RESPONSIBILITIES

Electronic Resources provided for use by Users are provided primarily for official and authorized Company business use and purposes in meeting business goals and objectives. Limited personal use of Electronic Resources is acceptable if it does not conflict with Company business and interests.

ATC assumes no liability for the personal, sensitive information that employees store on ATC systems or resources.

The use of Electronic Resources shall be in accordance with applicable local, state, and federal laws and regulations, as well as ATC's Code of Conduct.

1. **Access**

   Access to network resources and data is approved by data custodians, and access is granted by IT Cybersecurity.

   User Identification

   - Users must not share their personally assigned credentials, such as 'jsmith', for system access to ensure accurate accounting of user access and actions.
   - User IDs will be disabled within twenty-four (24) hours of notification of employee termination.

- Temporary User IDs (for testing, contractors/supplemental workers, and temporary employees) shall have an account expiration date that coincides with the anticipated end of employment, testing, or contract.

Authentication

- Refer to the Password Construction and Management Standard for technical password requirements.
- Acceptable use of passwords includes:
  - Always use different passwords for ATC accounts and non-ATC accounts.
  - Do not share ATC passwords with anyone, including administrative staff (Note: ATC staff will never ask you for your password). If someone demands a password, refer them to this document and direct them to IT.
  - Passwords should never be written down or stored online without encryption.
  - Do not reveal a password in email, chat, or other electronic communication.
  - Do not speak about a password in front of others.
  - Do not hint at the format of a password (e.g. "my family name").
  - Always decline the use of the "Remember Password" feature of applications.
  - Immediately change your password if you suspect it has been disclosed.

Authorization

- Users that are authorized to access Electronic Resources must comply with the following criteria:
  - Authorization must be approved by management, the data custodian or the system owner
  - User must be an active employee or contracted service provider to obtain and maintain access to authorized information
  - User may not share data or system access in any format with individuals that are not authorized to have access to the Electronic Resources

Privileged Access

- Users whose job duties require elevated or administrative rights to ATC systems must only use those elevated rights to perform necessary job functions, which must be aligned with this policy.

2. Remote Access

Remote access to Company information and systems shall be granted only to Users who require such remote access to meet an approved business need or perform prescribed job responsibilities. Remote access includes access to ATC's internal systems and access to applications provided through CONNECT.

- ATC provided devices should connect to ATC systems remotely through the CONNECT portal or the company VPN.
- Non-ATC device use can only connect to ATC resources through the CONNECT portal. (Note: section 12 of this policy covers ATC's 'Right to Monitor' devices connecting to Electronic Resources.
- An ATC Sponsor is required to request remote access for non-Company personnel and is responsible for ensuring that the non-Company remote access user is an active employee at their organization and all contracts between organizations are up to date.
- Non-company remote Users must be registered through the Contingent Worker process prior to being granted privileges to remotely access Company information or systems.
- All non-Company electronic equipment must adhere to the system and security requirements needed for remote access.

3. Hardware/Software

Users can only use the Company-provided version and configuration of browser and electronic mail software when using ATC-provided Electronic Resources.

If your ATC device is not available, ATC employees can use non-ATC provided electronic resources (e.g. home computer) to access applications provided through CONNECT.

All software (including Software as a Service), hardware (including Hardware as a Service and Infrastructure as a Service), and licenses used by the Company for ATC-owned electronic devices must be legally purchased or acquired through or approved by the IT Department with the collaboration of Supply Chain.

- Apple iOS Device Exception:
    - All ATC approved applications will be provided to the user for use on iOS devices.
    - Employees will not be reimbursed for any other software purchased on iOS devices.
    - Employees can install personal applications, but are not allowed to use those applications to store, process, or transmit any ATC confidential information.

Hardware is issued by the IT Department and equipment is not to be relocated/ reassigned without approval of the IT Department.

Personal devices may not be connected to physical networks.

Laptop Users that have a support role or participate in any disaster recovery/business continuity groups (IT, TERP, BCM, ATC Ready, BUCC) must take their laptops home at the end of each work day.

Users must be vigilant in providing physical safeguards to ATC equipment. Hardware must be stored out of sight when left in vehicles. Users shall lock the screens of the devices when leaving the device unattended and must also lock in a desk or filing cabinet all paper copies of ATC Confidential Information when not in use or whenever the user's work area is left unattended. Users shall be aware of their surroundings when accessing ATC Confidential Information in any format to protect from unapproved access, 'shoulder surfing,' or theft. Users must report lost or stolen devices as soon as possible. Refer to the Reporting section for further information.

4. Removable Media

The Company realizes that data needs to be shared/retained/stored using removable media to execute business processes and in preparation for business continuity or disaster recovery efforts. The Company realizes that certain business functions require retention of data on removable media, or data is backed up to removable media for Business Continuity or Disaster Recovery efforts.

- Data moved to removable media sources must be encrypted – please seek the assistance of IT Cybersecurity for encryption methods.
- All removable media devices must be physically secured when not in use and protected from theft when in use.

- The procurement and use of USB storage devices must be requested through the IT Service Desk. The IT Service Desk carries stock of Company-approved USB storage devices that are password-protected and encrypted.
- If an individual receives a USB drive from a vendor or finds a USB drive, s/he should not plug that USB drive into any ATC Electronic Resource. Please contact the IT Service Desk to have the USB drive scanned for malicious software.
  (Note: if your need for removable media allows for the storage of information online, consider the use of Microsoft OneDrive provided through our access to Office 365)

5. Web Browsing

Users have access to browse the internet while utilizing approved Electronic Resources. The Company limits or restricts certain categories of web sites that employees can browse while using Company-owned Electronic Resources. The categories are reviewed on a periodic basis, and changes to the blocked categories are approved by the Policy and Ethics Committee. Occasionally, legitimate sites are blocked and can be requested to be opened by submitting a request (including the business need) to the IT Service Desk and having the site reviewed by IT Cybersecurity.

Employee's utilizing ATC-provided equipment off the ATC network are encouraged to connect using ATC's VPN (e.g. remote.atcllc.com) to ensure proper network controls, filtering, and protection for the device.

6. Wireless Networks

The Company has provided a wireless network for employees to use, as well as a wireless network for vendors to use. Non-employees that need to access the Internet must use the vendor wireless network (RestrictedAccess). Non-employees are prohibited from accessing the Corporate network with non-Company owned computing equipment.

7. Mobility Security Guidelines

ATC provides mobile devices to those that have been approved to receive one and has outlined the usage of the electronic devices to protect ATC from the risk of compromised reliability, cyber security breach, and regulatory non-compliance. If you are a recipient of an ATC mobile device, you are responsible for reviewing the Mobile Device Management Standard.

If you are using a personal device to connect to ATC information you are responsible for reviewing and complying with the Acceptable Use of Personal Devices Policy.

8. Foreign Travel Computing

ATC permits employees who travel internationally for business or personal reasons to take ATC owned Electronic Resources with them. Employees are required to contact the IT ServiceDesk to provide notification of travel plans anytime ATC owned Electronic Resources will accompany the employee. Depending on the destination, you may not be permitted to take your standard ATC Electronic Resources. Please refer to the Foreign Travel Computing Guideline on Powerline for further information.

9. Cloud Computing

Use of a cloud computing service for ATC business must not commence until the formal evaluation process, as outlined in the Cloud Computing Procedure found on Powerline, has

been followed. Cloud computing-related risks must be properly documented, assessed, and managed.

10. Cyber Security

Users are expected to use and apply best practice cyber security measures (*e.g*., using complex passwords, avoiding unsolicited executable files, not introducing plug and play devices to the environment, etc.) in their use of systems and devices. Cyber Security practices change with time, and Users will be provided opportunities to stay current on best practices through available Company communications and training.

Users are required to report all suspicious emails and other suspicious computer activity to IT Security or the Service Desk for review. If you See Something, Say Something.

The following are recommendations for employees to follow to maintain good cyber security practices:

- Users must exercise caution to avoid divulging proprietary or confidential information about ATC.
- Users may not share specific methodologies or technologies utilized to perform certain job duties, although it is acceptable to share industry certifications achieved.
- Users should not click on any unsolicited ads, emails, or attachments. These may contain malicious programs that are capable of recording passwords, usernames, or other confidential information.
- Users should not save login information in the browser or share phone numbers, addresses, or passwords. This information could be used to impersonate a company employee and be exploited to gather sensitive company information.
- Users should not enter personal or company information into any pop-up windows. Even though some pop-ups may look legitimate, they may instead be used to collect information for malicious purposes.
- Users are encouraged to not use their ATC e-mail address when providing their e-mail address for non-ATC purposes. Examples include online shopping and social media usage.

11. Right to Monitor

The Company reserves the right to monitor and review all activities and messages using Electronic Resources. Consistent with federal and state law, all electronic records can and will be monitored, retrieved, and disclosed as necessary to protect the company's business purposes, which include ensuring that the electronic communication technology is not being abused.

- The Company reserves the right to disclose the nature and content of any User's activities involving Electronic Resources to law enforcement officials or other third parties without any prior notice to the User.
- Users should have no expectations of privacy when using Electronic Resources.
- All Electronic Resources and all messages created, received, processed, transmitted, and/or stored on Electronic Resources are Company information assets and property.
- The Company reserves the right to remove any non-standard corporate software, or any software that does not comply with the Company's existing licensing agreements
- The Company reserves the right to remove any non-ATC owned devices from any corporate networks or computers.

- The Company reserves the right to perform electronic discovery (legal discovery) of ATC-owned and non-ATC owned Electronic Resources that store ATC information.
- The Company reserves the right to take possession of Company Electronic Resources at any time.
- The Company reserves the right to monitor non-company electronic resources while accessing ATC systems and information.
- While ATC has the right to log and monitor your activity on ATC assets and systems, ATC will not view personal, sensitive information that you provide to external websites, such as financial or health information.

12. Prohibited Conduct

Conduct that is prohibited and that may result in disciplinary action, up to and including termination, includes but is not limited to the following:

- Use of Electronic Resources that is illegal, is a conflict of Company interest as defined by ATC's Code of Conduct, violates ATC policy, or interferes with business operations and ATC's ability to deliver services to its customers.
- Storing ATC Confidential information, including e-mail messages or calendar invites to personal accounts (*e.g.*, Gmail, Hotmail, Yahoo) or non-ATC Electronic Resources.
- Linking, bookmarking, accessing, downloading, transmitting, or storing Objectionable and/or illegal material, images, or content.
- Use of Electronic Resources to conduct personal or non-Company sales or other business transactions, except for using the internal Classifieds board on Powerline.
- Participating in any Objectionable chat groups, electronic bulletin boards, or forums.
- Using features that automatically forward electronic mail messages.
- Allowing others to access the Internet through ATC's network or ATC's Electronic Mail Resources by using their accounts.
- Using software or features (such as an anonymous mail sender) that obscures or masks the identity of the message sender.
- Purchasing of software and hardware by non-IT employees.
- Sharing ATC Confidential Information with parties that are not authorized to have access to such information.
- Adjusting the operating system, browser, antivirus, encryption, monitoring, content filtering or electronic mail software security settings to be less restrictive than the Company-approved configuration.
- Using non-approved external web sites for transferring ATC Confidential Information. This includes, but is not limited to, sites like personal webmail accounts (*e.g.*, Gmail), social media sites (*e.g.*, Facebook), Software as a Service (*e.g.*, Google Apps) and file sharing web sites (*e.g.*, Dropbox).
- Using web sites known as "Remote Access Tools" for the ability to log into your work computer from any external computer (*e.g.*, GoToMyPC)
- Connecting personal mini storage cards, USB mass storage devices (including thumb drives, cell phones, digital cameras, mp3 players, etc.) or other electronic devices (wireless routers, computers) not owned by ATC to any ATC network or their Company-owned equipment for any use other than to recharge the battery or sync personal media files. Please reference the Mobile Device Management Standard for more details.
- Receiving or copying unauthorized copyrighted software, content and/or licenses for corporate use, personal use, or for distribution to others.

- Use of elevated or administrative rights outside of necessary job functions, including but not limited to: installing unapproved software, modifying security settings, modifying approved configurations, or creating credentials and/or accounts that have not been authorized.

REPORTING

The requirements of this policy, although specific, should not be considered a comprehensive listing. The Company considers consistency with requirements as the basis for considering the appropriateness of other activities and practices that are not specifically addressed.

Report the following to the IT Cybersecurity Team (608-877-8180 or ITSecurityTeam@atcllc.com) as soon as possible:

- Actual or suspected misuse of Electronic Resources
- Upon the receipt or continued receipt of Objectionable content
- Lost or stolen electronic devices

It is the responsibility of all ATC employees 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.

Employees and 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; forming, joining or supporting labor unions; or bargaining collectively through representatives of their choosing.