Policy Owners:	Executive Vice President, CFO & Treasurer
Original Issue Date:	5/14/18
Revision Number:	0
Revised Effective Date:	N/A
Approved By:	Policy & Ethics Committee

ACCEPTABLE USE OF PERSONAL DEVICES POLICY

PURPOSE

Some employees with ATC-owned smartphones seek the convenience and simplicity of using their personal smartphone to access ATC information and systems. This policy provides rules of behavior in the use of personally-owned smart phones and/or tablets by American Transmission Company ('ATC' or the 'Company') employees and contingent workers which are used to access ATC information and systems. Access to, and continued use of, network resources is granted on condition that each user reads, respects, and follows ATC's policies concerning the use of these devices, information, and services. Participation in the use of this personal device option is voluntary, and employees will not be required to use their own device to connect to ATC information, systems, or networks.

SCOPE

This policy applies to all employees and contingent workers who use their non-ATC owned smartphones and/or tablets to connect to ATC information, systems, or networks for ATC business purposes.

DEFINITIONS

Biometric Protection – Using the unique characteristics of a person (voice pattern, fingerprint, retina pattern, etc.) to allow or deny access to a system or device.

Contingent Worker – Any contractor, consultant, or service vendor/provider, including local distribution companies, and their employees contracted to perform work for ATC. These individuals are not employees of ATC and are not eligible for benefits offered by the Company.

Jailbroken (Rooted) – The condition that a device is in when the software restrictions put in place by the manufacturer (Apple, etc.) have been removed. This provides "root" access to the device, allowing installation of unapproved applications and modification of the devices defaults.

Personal Device – A device that is not owned by ATC.

Smartphone – A mobile phone that performs many of the same functions of a computer, typically having a touchscreen, internet access, and an operating system capable of running downloaded applications.

Tablet – A portable PC with a mobile operating system and a touchscreen display.

RESPONSIBILITIES

Employees and contingent workers are responsible for:

- Treating all ATC information in accordance with ATC's Acceptable Use of Electronic Resources Policy.
- Reporting any lost, stolen, sold, or repurposed device that has been granted access to ATC-owned information to the Service Desk as soon as possible (within 24 hours).
- Paying the costs associated with their personal device, including but not limited to data usage costs and any repair or replacement costs.
- Maintaining a device that supports all required security configurations including screen lock with password or biometric protection, inactive device lockout, and encryption.
- Understanding and abiding by the following, should they elect to utilize a personal device for Company business:
    - While the Company 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.
    - The Company may be required, in the event of a lawsuit or investigation, to preserve, collect, and analyze ATC-related communications, including documents, e-mails, text messages, and voicemails. As long as an employee keeps business and personal items separate, ATC can preserve and collect Company information without access to an employee's personal device or information. ATC will give employees tips on setting up their personal devices to preserve this separation, such as a business-only phone number for calls and texts. If an employee elects to mix personal and business items using, for example, the employee's personal phone number to conduct ATC business, the employee understands that ATC may need access to that information one day.

Information Technology is responsible for:

- Providing the necessary mechanisms to connect to allowed ATC resources.
- Maintaining a list of acceptable devices with their minimum configuration and control requirements.
- Providing support for any ATC-owned or required application, including connectivity and access, provided the device meets IT-defined specifications. Note: While ATC IT support is generally limited to ATC-owned devices and applications, IT will attempt to facilitate employees' use of personal devices under this policy by providing baseline support of the related tools utilized.

Prohibited Conduct:

- Altering or removing security-related applications and configurations put in place to protect ATC information without approval.
- Connecting a rooted or jailbroken personal device to ATC resources
- Connecting personal devices and software that do not meet the minimum requirements to ATC resources
- Installing an application on a personal device from an unofficial source. Note: Official source examples include the Apple store for Apple device applications, the Microsoft store for Windows phone applications, and the Google Play store for Android device applications.

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.

EXCEPTIONS/VIOLATIONS

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

The Company reserves the right to remove any ATC-owned or required information / applications from personal devices for violating this policy.

The Company reserves the right to refuse the ability to connect personal devices to ATC-owned or required information / network if the device is in violation of this policy.

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