**Traveling with Technology Procedure**

Employees of the **[Organization]** will have occasion to travel outside of the secure **[Organization]** network as part of their job responsibilities, and may be required to bring **[Organization]** technology resources.

# Purpose

The purpose of this procedure is to assist an **[Organization]** employee in traveling safely, and giving guidelines for connectivity, physical security and data security. While these guidelines are for **[Organization]** -owned equipment, they can also be applied to personal devices as a best practice.

# Scope

All staff, employees and entities working on behalf of **[Organization]** that travel are subject to this procedure.

# Procedure

Pre-Travel:

* If possible, create a Service Desk request for a VPN account two (2) weeks before the scheduled departure date if you have need to access content that resides on the **[Organization]** network outside of your web-based Office 365 account.
* Ensure that the operating system has been updated to current **[Organization]** patch levels. If you have any questions, please call the Help Desk for assistance, **xxx-xxx-xxxx**.
* Ensure that Endpoint Protection (System Center Endpoint Protection) has been updated with the latest available definitions. If you have any questions, please call the Help Desk for assistance.
* If traveling by air, check the Transportation Security Administration website ([www.tsa.gov](http://www.tsa.gov)) for any regulations that may apply to the types of technology with which you are traveling. (An example is the emergency ban on Samsung Galaxy Note 7 devices.)
* If traveling internationally, please refer to the Wassenaar Arrangement website ([www.wassenaar.org](http://www.wassenaar.org)) regarding regulations about traveling with encrypted devices. All **[Organization]** laptops have their hard drives encrypted, so ensure that the country you are traveling to allows encrypted devices to cross their border.

In transit to destination:

* If traveling via airplane with a laptop, please do not check it in and keep track of it among your carry-on items. This is a TSA recommendation.
* At any TSA checkpoint, laptops and mobile devices go in separate bins and may or may not be swabbed with chemicals.
* Please comply with any in-flight instructions regarding technology use, including setting cellphones and tablets to airline mode.
* If renting a vehicle that uses Bluetooth technology, sync your devices at your own risk.

While staying in accommodations:

* Try and keep your mobile devices with you at all times. If you must leave them in your room, power them down and store them securely whenever possible.
* If you must leave the room with the device on, please lock it at minimum.
* If using the wireless connection provided by the hotel, ensure that you are connecting to the correct wireless SSID (the name of the wireless network) and the current password. Please scrutinize the name, as rogue access points with similar names can be utilized to listen in on your connection and steal your data or passwords.
* If accessing the **[Organization]** network remotely, be sure to immediately connect to your VPN account once your secure wireless connection has been made. This action will create a VPN tunnel to encrypt all traffic which will keep the data exchange secure.

While attending conferences or meetings:

* Do not leave your device unattended whenever possible.
* If there is a break where the room is left unoccupied and locked, please lock or shut down the device if it must be left unattended.
* Avoid using shared computers or kiosk machines; if you must use a shared computer or kiosk machine, avoid using any website that requires a password. If you do not have an option and have to input a password at a shared computer, make sure to you log out of any websites that required your login credentials.

Upon returning from travel:

* When returning any rental car, ensure that any synced devices are deleted prior to returning the keys.
* Initiate a full virus scan on your laptop; if you need assistance in accomplishing this, please call the Help Desk.

# Enforcement

This procedure is for your protection. Violation of this procedure could be reported to the appropriate supervisor and could be subject to potential disciplinary action, up to and including termination.

# Exceptions

# Limited exceptions to the procedure must be approved by the [management].

1. **Definitions**
* Endpoint Protection (also Endpoint Security): Software installed on all machines designed to protect it from malicious software and intrusion attempts. **[Organization]** currently uses System Center Endpoint Protection.
* VPN (Virtual Private Network): A method for securing communications by creating an encrypted ‘tunnel’ to protect data and communications.