**International Travel Remote Access**

**Policy**:

The purpose of this policy is to provide guidance to offices supported by the Summit County Office of Information Technology (OIT) when personnel from that office need to travel to territories outside of the USA and Canada with the ability to connect to County of Summit Ohio (County) equipment, systems and/or data remotely to conduct County business.

**Remote Access Procedure**:

For the protection and confidentiality of County systems, data, and staff, this procedure is to document the necessary steps to effectively provide the traveling personnel remote access to the county systems, data, and/or devices.

**Procedure summary**:

1. International Travel Remote Access Request Form
2. Traveling personnel’s responsibilities
3. Travel device requirements
4. OIT responsibilities

**Procedure detail**:

1. Complete an International Travel Remote Access Request form that:
	1. Shall be submitted to OIT at least 30 days in advance via OIT’s Service Portal
	2. Shall not be approved until acknowledged in writing by their Department Director, The County CIO, and The County Law Director
	3. Shall provide a complete list of dates, times, and expected destination country(ies)
	4. Shall include the serial number and basic description of device(s) seeking approval to travel with
	5. Shall authorize for travel *only* electronic devices that are fully documented on this form (includes mobile phone, laptop, tablet, MFA token, USB/flash drive)
	6. Shall require the traveling personnel to agree to the terms and conditions
2. Traveling personnel’s responsibilities:
	1. Promptly notify their supervisor and OIT of any unexpected travel changes or delays that may affect access requirements
	2. Promptly notify their supervisor and OIT if they become aware of information or data pertaining to the County that they may have revealed whether accidentally (i.e. realized that someone may have shoulder surfed), or intentionally (i.e. compelled by Customs/Border Control to reveal password(s), encryption key(s), MFA token(s), and/or relinquish equipment for inspection)
	3. Promptly notify their supervisor and OIT if any equipment is lost or stolen.
	4. Promptly change their password(s) upon return to the USA
	5. Promptly return temporarily assigned travel equipment to OIT
	6. Use the County issued device(s) for business/work purposes only
	7. Acknowledge that this policy applies to all county issued devices that may store or connect to County data, as well as any non-county issued devices that may contain County data, including desktop PC, laptop PC, iPad, iPhone or other mobile computing device, as well as external storage devices such as flash drives, external HDD/SSD, etc
3. Travel device requirements:
	1. Require multifactor authentication
	2. Require full disk encryption with at least AES-256 level encryption
	3. Require a local software firewall that blocks all inbound sourced traffic from local networks
	4. Be managed by a remote or mobile device management system that allows triggering of remotely wiping all data from the device
	5. Support device authentication for corporate VPN access
	6. Require all Internet access to go through the corporate VPN (no split-tunnel DNS, pre-login authentication)
	7. Require BIOS/firmware password to be configured with a password matching County password requirements
	8. Require boot sequence to be restricted to only the primary internal storage device
	9. Administrative credentials shall be cleared from the local device cache (erase unnecessary cached user profiles)

NOTE: Any storage device containing or potentially containing county data must have at least AES-256 level encryption protected by a password matching County password policy requirement (15-character min, complex, unique) and/or an approved biometric sensor.

1. OIT responsibilities:
	1. Prepare and provide travel equipment to the traveling personnel in advance of travel
	2. Provide training/instruction for devices such as laptops or encrypted external storage devices as well as things to watch for and reporting procedure while traveling
	3. Ensure that all travel device serial numbers are accurately documented, including adding the assigned travel equipment to the form
	4. If required, create time-restricted network access rules to allow VPN activity from the device during the designated travel window
	5. Confirm that the traveling personnel change their password upon returning to the USA
	6. Erase the equipment approved for travel and return to factory default or County baseline image.
	7. Remove any access rules exceptions created for the travel request
	8. Promptly disable relevant access and trigger remote device wipe upon report of stolen or lost equipment.