Traveling With Technology – Best Practices for Michigan Tech Employees

Before You Leave

- **Less is More** – take only what you absolutely need in terms of technology and make efforts to consolidate devices and data – you'll thank yourself when you're in a bustling train station, airport, or hotel lobby.
- **Update** – If you'll be taking personal devices, ensure all technology devices are patched/updated to the most current software available
- **Use Loaner Devices** – strongly recommended for any international travel; required for travel to high-risk countries. If you're not using loaner devices, make sure that your devices are configured to encrypt data at rest.
- **Don't Take Unnecessary Data** – Ensure there is no EAR or ITAR-controlled or highly restricted technical data on your device. Don't carry data you don't want others to see, e.g., data files from your research, financial information, medical records, photos.
- **Verify** – before departing, make sure you have the data, software, and access you need whether on a work, personal, or loaner device. Make sure you've securely removed data not pertinent to your planned travel.
- **Backup** – retain a copy of any data you're traveling with on a non-travel device in the event your device is lost or stolen; make sure you have scanned copies of important travel documents (passport, visas, etc.) and ideally ensure they're in a cloud location accessible to you while traveling.
- **Change Your Passwords** before leaving if you expect to use public wifi or computing resources or if you will be entering your password in an area where others may be able to view or record it.
- **Disable Services** – if you don't need to use file or printer sharing, or Bluetooth or other wireless services while traveling, disable them before you leave. You should also disable any automatic Wifi connection if your device supports such.
- **Register Your Travel** on the Michigan Tech International Travel Registry and verify export control requirements; note that MTU's major online services may work differently or not at all depending on the country(ies) you're traveling to. Details for Canvas, Duo Security, Google Workspace, Microsoft Online Services, and Zoom can be found at their respective links.

While Traveling

- **Carry On** technology devices - never pack them in checked luggage
- **Power Off** technology devices before you transit an international border crossing –devices can be powered back on after you have been admitted to the country.
- **Keep** your technology devices with you whenever possible; when not, use a hotel-provided safe.
- **Use Caution** with Wifi – avoid if possible (use tethering on your smartphone instead), use VPN if permissible in your travel areas. You should avoid accessing confidential systems/services when using public Wifi.
- **Never Connect** unknown devices/plugs (incl. power points at hotels or airports) – use a power bank or charging cable and plug that you own
- **Never Login** or access confidential information from public computers; if you must download files on a public computer, be sure to permanently delete them before ending your session.
- **Beware** of shoulder surfing – particularly if using technology in an airplane or at a conference; lock your device whenever you're not actively using it.

Before You Return

- **Consider** whether social media applications should be deleted – you can always reinstall them later and generally have all content restored.
- **Be Aware** that US Customs and Border Protection (CBP) officers have the authority to search and retain devices of anyone entering the United States, including without probable cause. Fully cooperate with CBP. If you have a University device, give them your device password if asked. If they retain your device, get a receipt with contact information to arrange for its return. If you have a personal device:
    - If you are a U.S. citizen or a lawful permanent resident, law enforcement may not deny entry for refusing to supply a password or unlock a device. However, doing so may lead to additional delays, questioning, and seizure of the device.
    - If you are not a U.S. citizen or lawful permanent resident, you may be denied entry for your refusal to provide a password.

After You Return

- **Change Password(s)** – We strongly recommend that you change any passwords you used while traveling, but at a minimum any that were used without an active MTU VPN connection.
- **Report** – report your travel if required to Research Security (researchsecurity-l@mtu.edu), and report any suspicious activity or tampering with your technology devices to Information Security and Assurance (security-l@mtu.edu)
- **Return** – return any loaner device(s) to Michigan Tech IT after you've copied any data or files you need off the device(s). Devices returned to Michigan Tech IT will have all data securely deleted before the devices are reused.