Digital Security Guidelines for Travelers

Low Risk Travel and Safe Computing Best Practices

- Install all the latest security updates on your devices.
- Do not reuse passwords. Use unique passwords for each of your important Online services.
- Use strong passwords for your important Online services, including your Middlebury account.
- Ensure that you are setup for Multi Factor Authentication (MFA) http://go.middlebury.edu/mfasetup
- Never leave your devices unattended. Theft of phones, laptops, and tablets is all too common, even close to home.
- Secure your phone or tablet with a PIN or passcode. If you do lose access to your device, a passcode or PIN will help protect your accounts and information from prying eyes.
- Ensure encryption is enabled on your devices. Using a PIN on iOS is all it takes to encrypt your device.
- Do not use hotel or public Wi-Fi to perform sensitive tasks, such as those concerning Personally identifiable information, payment card information, or other protected information types.
- Pay close attention to web browser security warnings. Warnings that your “connection is not secure” could indicate that someone is attempting to steal your password and data.
- Do not use shared or public computers for sensitive work. Keyloggers installed on hotel computers are another frequent source of password theft.
- Report lost or stolen devices to ITS immediately: 802-443-2200, helpdesk@middlebury.edu.
- If you have an Information Security incident, or have questions about Information Security before traveling, please reach out to infosec@middlebury.edu

Medium Risk Travel

- Where possible, remove sensitive data from your device before traveling. If there is no sensitive data on your device to begin with, you will have much less to be concerned about should your device go missing.
- Shift sensitive data to the cloud. “Travel light” by moving sensitive data to MiddFiles/MIISFiles, your Middlebury OneDrive, or Middlebury’s Google Drive.

High Risk Travel

- Phones, computers, and tablets may be searched without your consent or knowledge.
  - All data stored on devices you travel with may be scanned, copied, and tampered with.
- Do not bring your daily use phone, laptop, or tablet to a high-risk location.
- Make use of Middlebury owned “burner” devices, i.e. temporary use-only phones, laptops, and/or tablets. Contact ITS to obtain such a device.
- Upon return, at a minimum, do a complete traveled with, restoring your data and apps from your cloud services. “Reset to factory defaults” on any devices you traveled with, restoring your data and apps from cloud services.