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 really important online services, including your Middlebury account.
- **Enroll in Multi-Factor Authentication.** Visit http://go.middlebury.edu/getmfa to sign up today.
- **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.
- **Enable encryption 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**, including checking email. Use your phone's cellular data plan when necessary and/or consider a commercial VPN option (see below).
- **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.
- **Use a commercial VPN service for sensitive tasks.** A commercial VPN can help protect you from *man-in-the-middle* and other network eavesdropping attacks designed to steal your data.
- **Report lost or stolen devices to ITS immediately:** 802-443-2200, helpdesk@middlebury.edu.

Medium Risk Travel

- **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.**
    - **Any and all data stored on devices you travel with may be scanned and copied.**
    - Any **devices left unattended may be tampered with**, perhaps in undetectable ways.
- **Do not bring your daily use phone, laptop, or tablet to a high risk location.**
    - Leave your personal devices at home.
    - Leave Middlebury devices at home.
- Make use of "**burner" devices, i.e. temporary use-only phones, laptops, and/or tablets**.
- Create a **burner email address** for use while you are travelling. Your primary accounts will be vastly more secure if you simply avoid accessing them in high risk areas.
- Upon return, at a minimum, do a complete **"reset to factory defaults**" on any devices you travelled with, restoring your data and apps from your cloud services.