Dear Traveler,

Along with the tremendous rewards of international travel, we face a number of hazards. These hazards include technology and identity theft. The theft of personal information may damage you personally or financially. Allowing sensitive information or research to be disclosed while abroad may violate U.S. export control laws. Violations can subject you as an individual and the University as an institution to possible criminal and civil penalties. The following tips will help minimize your risk. If you have any questions about these guidelines, please contact Scot Allen or Claire Calhoun in Secure and Global Research at +1 (970) 491-1563 or vpr_export_control@colostate.edu.

Must consider:
- Are you taking or shipping any specialized equipment or materials that might have military or dual military-civilian use?
- Are you taking any export-controlled technical data, for example according to contract terms?

If so, please contact CSU export control (above) as you may need prior federal approval.

Best practices:
- When you are taking a laptop, tablet, or smartphone, ask your IT group if they may be able to loan you a clean machine, from which you could check email or finalize your conference presentation, but that would not include any restricted software or data, and that they could scrub upon your return.
- If possible, send your presentation ahead, access materials through a secure browser on your device, or take only a flash-drive containing relevant information.
- Update all software and apps before you go. Do not update apps or allow changes to your computer through internet connections abroad. The FBI has identified malicious software disguised as updates to legitimate software.
- Avoid local networks that may introduce malware, capture usernames and passwords, or download your contacts and personal info. Use a cellphone data plan instead if possible.
- Use password protection on devices to limit access without your knowledge. Turn them off when not in use.
- CSU recommends that you take only the information you need, and remove personal information you would not want publicly disclosed.
- Some licensed software on your laptop or accessible through a virtual machine may be restricted for use when traveling abroad, by the terms of the software license agreement.
- Keep your electronic equipment with you at all times to avoid tampering.
- Be aware that laptops and phones are subject to search at international borders.

When a CSU traveler carries certain information or software to another country on a laptop, tablet, or phone, federal agencies consider the information or software exported to that country, even if not actively used in a presentation, discussion, or research while abroad.

For more information about travel to your destination, please consult these resources:
State Department country information: https://travel.state.gov/content/passports/en/country.html
Smart Traveler Enrollment Program (STEP), register with the US embassy: https://step.state.gov/
Commerce Department Country Commercial Guides: https://www.export.gov/ccg
Centers for Disease Control and Prevention (CDC) Travel Health: https://wwwnc.cdc.gov/travel

If you have any questions or concerns, please contact Scot Allen or Claire Calhoun in Secure and Global Research at +1 (970) 491-1553 or vpr_export_control@colostate.edu.
For more information, consult https://www.research.colostate.edu/sgr/.