Information Security Office

ISO Position Paper

Position Title	Personal Devices in China
Position Audience	Princeton University Community
Contact	Information Security Office: InfoSec@princeton.edu
Position Release Date	July 30, 2020
Last Update	Initial posting

Problem Statement
With the University addressing the impacts of COVID-19, the Graduate School is assessing how they may allow some of their international graduate students to start their programs remotely for the fall semester. In particular, some of the University's engineering and sciences programs have large numbers of students in China who will need to remain there and require access to University systems.

Disclaimer
Please be aware that there is little that Princeton OIT can do to support personal devices on networks in China. We do our best to support Princeton international travelers with loaner devices and temporary email addresses, but for residents we have no solutions beyond best practices and vigilance.

Baseline Assessment
- No device can be protected against all possible forms of system and information compromise, especially when in countries that are deemed as high risk.
- You must assume that any device in a high risk country will be compromised in some, potentially undetectable way.
- You must realize that connections will be poor, inconsistent, and perhaps non-existent.
- You must realize that the computing environment is constantly changing in China.
- The biggest issue is oftentimes less about security of devices and more about accessibility to western resources.

ISO Position
The ISO recommends you follow these best practices.

Security Best Practices When Connecting to Princeton:
- Always use the Princeton virtual private network (VPN) solution (GlobalConnect).
- Use two factor authentication (2FA) whenever possible.

- Graduate students should have access to any Princeton solutions that they require, which may include Zoom, Box, Google Drive, and the learning management system (LMS) used by the graduate school.
- Always have an active and up to date virus protection solution on your device.
- Utilize the Princeton password manager (Lastpass).
- Never store Princeton data on Chinese-managed cloud services.
- Be careful about what you post about Princeton on social media, particularly Chinese social media.

Security Best Practices in High Risk Countries:

- Configure a firewall to block incoming connections.
- Turn off file and printer sharing.
- Disable any remote desktop software.
- Disable bluetooth when not in use.
- Avoid public wifi and public hotspots. Use VPN if use of public wifi or hotspots is unavoidable.
- Use trusted wifi instead of cellular data whenever possible.
- Understand the sensitivity of your data.
- Beware of your surroundings when logging in or adding data to your device.
- Be discerning on how your device and/or account is behaving, and report any unusual issues or behaviors to the OIT Support & Operations Center (1-609-258-4357 or helpdesk@princeton.edu).
- Visit the ISO's Safe Computing page for additional information about the above topics as well as other information security topics (https://princeton.edu/safecomputing).

For Further Guidance

Questions and clarification can be provided by contacting the Information Security Office at infosec@princeton.edu.

Information Security Office
Princeton University

Data classification: Public