Information Security Office

ISO Position Paper

Position Title	Remotely connecting to University systems
Position Audience	All employees
Contact	Information Security Office: InfoSec@princeton.edu
Position Release Date	November 15, 2017
Last Update	March 13, 2020

Problem Statement

Members of the University community have inquired about remotely accessing University systems using their personal devices.

ISO Position

It is the position of the Information Security Office that remote access to University systems is only through approved University devices. Personal devices introduce security risks to the University infrastructure and data, and should not be used to access your work computer, or University files and applications.

For both security and business continuity reasons, University-issued laptops should be used when working remotely.

Special note as of 3/6/20: In view of the impending challenges with respect to the COVID-19 virus and the need to work from home, the ISO is relaxing its position on the usage of personal devices for University work during this crisis. As long as the personal device is running a supported operating system with an active firewall and antivirus software, it is acceptable to use these devices until further notice.

AV software
- **Windows**
- **Mac**
- **Android**
- **Apple iOS: Not applicable**

Enable firewall
- **Windows**
- **Mac**

Supported operating systems
- **Windows**
- Mac OS: High Sierra, Mojave, Catalina
- iOS: 12.4.5 and up
- Android: 8.0 and up