ISO Position Paper

<table>
<thead>
<tr>
<th>Position Title</th>
<th>Remotely connecting to University systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Position Audience</td>
<td>All employees</td>
</tr>
<tr>
<td>Contact</td>
<td>Information Security Office: <a href="mailto:InfoSec@princeton.edu">InfoSec@princeton.edu</a></td>
</tr>
<tr>
<td>Position Release Date</td>
<td>November 15, 2017</td>
</tr>
<tr>
<td>Last Update</td>
<td>March 13, 2020</td>
</tr>
</tbody>
</table>

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

Information Security Office
Princeton University

Data classification: Public