IU has a new policy (IT-12.1) which outlines security requirements for laptops and other mobile devices. The policy can be reviewed at [https://protect.iu.edu/online-safety/policies/it121.html](https://protect.iu.edu/online-safety/policies/it121.html).

All systems and mobile devices, including devices that are personally owned, must comply with IU requirements in order to be used for university business.

### Laptop/Mobile Device Requirements

<table>
<thead>
<tr>
<th>Table of Required Safeguards by Device Type</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mobile</strong></td>
</tr>
<tr>
<td>Handheld mobile device (i.e., Smart Phone, Tablet, etc.)</td>
</tr>
<tr>
<td>Laptop/Notebook Computer</td>
</tr>
</tbody>
</table>

[2] Remember that use of mobile devices to access, store, manipulate critical information requires written approval from a senior executive of the unit or the IRB and encryption on the device and in transit.

[3] See KB article on Passwords and Passphrases: [https://kb.iu.edu/data/acpu.html](https://kb.iu.edu/data/acpu.html)

### Required Actions

- Use a **whole-disk encryption** program on all laptops and mobile devices. For more information: [http://kb.iu.edu/data/bcnh.html#laptop](http://kb.iu.edu/data/bcnh.html#laptop)
- Maintain all software and mobile devices with the latest vendor recommended updates. Note: PCs must have Windows 7.x or later since earlier versions such as Windows XP do not have the necessary safeguards in place. IU recommends Secunia PSI for software updates. For more information: [http://kb.iu.edu/data/azfj.html](http://kb.iu.edu/data/azfj.html)
- Run **anti-virus software**. For more information: [http://kb.iu.edu/data/agpp.html](http://kb.iu.edu/data/agpp.html)
- Use **Virtual Private Network (VPN)** or login through IUanyWare when working remotely. For more details, please review the kb articles referenced on the left.
- Do not store critical data on personal storage mediums such as flash drives, disks or local drives.

*For questions regarding laptop and mobile device requirements you may contact your LSP.*

Revised 9/2015