Top 10 Information Security Tips for Penn Faculty
Developed by the Office of Information Security

1. **Know where to get help** – Get to know your Local Support Provider (LSP). For more information see: http://www.upenn.edu/computing/view/support/faculty.html

2. **Practice “good hygiene”**
   a. **Keep your operating system and applications up to date** with patches (enable “auto-updating” whenever possible).
   b. **Turn on your systems firewall.**
   c. **Install anti-virus software** and keep it and its virus definitions up to date. Penn makes this very easy to do by providing licenses for Symantec Anti-Virus (SAV) for your work and personal computers (PC’s and Mac’s) at no cost. See Security Application section: http://www.upenn.edu/computing/product/.

3. **Use strong, unique passwords** (for your computers, and for systems like PennKey and Facebook) and don’t ever share them with anyone.

4. **Eliminate PII** – Purge all sensitive data (SSN’s, credit card information, student records, health information, etc.) from your computer unless it is absolutely necessary. Your LSP can help you automate the process of finding sensitive data using special software.

5. **Be wary of unsolicited links or attachments** - Be suspicious of links or attachments delivered via email that you didn’t ask for. Check with the sender before opening them or use other methods to ensure they are benign, like searching for the same content yourself independently online or scanning attachments with your anti-virus software.

6. **Be alert for “phishing”** – Phishing refers to a specially crafted e-mail from an attacker that looks legitimate in an effort to trick you into divulging personal information. For more information on detecting and avoiding phishing attempts see: http://www.upenn.edu/computing/security/advisories/phishing.php

7. **Not all wireless connections are equal.** AirPennNet provides secure authentication and encrypted traffic. AirPennNet-Guest provides secure authentication, but does not encrypt your traffic. Unencrypted traffic means that a malicious user could potentially sniff your email and web data as it is delivered to your computer (depending on your applications settings). Lastly, public wireless hot spots, such as offered at web cafés and coffee shops, may have an even larger untrusted community and pose even more risks. Know your wireless networks and use encrypted services whenever in doubt (e.g., HTTPS over HTTP when web-browsing).

8. **Protect research data** – The requirements for data manipulation, collaboration and publication impose unique risks on research data. Make sure to securely backup your data in case of corruption or loss, and to encrypt it when transmitting or shipping it if it contains PII. Maintain awareness of any federal requirements for data protection, storage and accessibility as well. When in doubt, your LSP can help.

9. **Beware the cloud** – Cloud services provide new and exciting opportunities to communicate, collaborate, and compute. Unfortunately, they also introduce compliance and other risks. Familiarize yourself with the Cloud Guidance document and contact your LSP for questions and assistance: http://www.upenn.edu/almanac/volumes/v56/n27/cloud.html

10. **Protect Student Data** - The University’s Policy on the Confidentiality of Student Records - which incorporates the federal Family Educational Rights and Privacy Act (FERPA) law - provides the most directly relevant rules on the protection of student data: http://www.upenn.edu/almanac/volumes/v56/n25/confidentiality.html. If you need assistance contact your LSP or the University Privacy office at privacy@upenn.edu

---

For more information and resources please see the Information Security website at http://www.upenn.edu/computing/security, or contact us at security@isc.upenn.edu or 215-898-2172.