Top 10 Information Security Tips for Penn Staff
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/staff.html](http://www.upenn.edu/computing/view/support/staff.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/](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. **Lock/log off systems** - Always lock or log off your computer and log out of applications before walking away from it.

6. **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.

7. **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](http://www.upenn.edu/computing/security/advisories/phishing.php)

8. **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).

9. **Take extra care with portable devices:** Be especially careful about what data you store on portable devices, like laptops, thumb drives and smartphones. These are more easily lost and stolen and may require extra protections, like encryption or remote file deletion.

10. **Be careful what you share on Social Media** (like Facebook, Twitter, etc.) – it represents a powerful and exciting new set of technological tools and resources. However, these services also present new risks. Be aware that anything you share can be preserved online indefinitely, and be rapidly shared beyond your original intentions.

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