1. **Use strong, difficult-to-guess passwords on computers, mobile devices and other password protected media**
   - Anyone who knows or can guess your password can see or do whatever you can.
   - Passwords should be at least 10 characters, and include a mix of letters, numbers and symbols.
   - NEVER use a password commonly tried by hacking tools:
     - A blank or trivial password (e.g., password, passwd),
     - A password set to its initial or default value,
     - A simple sequence (e.g.,12345678, qwerty, abc123),
     - A word in the dictionary of any language,
     - A word with obvious substitutions (e.g., p@ssw0rd),
     - An unaltered well-known quote, title, lyric, cheer, or
     - Your user ID or a public piece of information about you or your family (e.g., name, birth date, school, team).
   - Use different ID and password combinations for different websites.
   - Phrases can be the basis for an effective and easy to remember password, e.g., "I am one happy person at Princeton University!" could become the password "Im1hp@PU!" ***(Please do not use this or any other password shared as an example in any document.)***
   - Do not share your passwords with others.
   - Change your password regularly to limit the time a hacker has to discover it.
   - Restrict what you share on social media sites. The data you enter may be used to successfully answer test questions used to do a password reset.
   - Avoid writing passwords down, but if you must, mask it, keep the piece of paper in a safe place and do not include related data (e.g., ID, site name).
   - Commercially available password management software can keep your passwords in an encrypted, password-protected file either locally on your computer, or in the "cloud" to allow you to share passwords among multiple computing and mobile devices. Consult with your IT support person or the OIT Help Desk at (609) 258-HELP to ensure that you select an effective, secure product.

2. **Ensure that vendor software updates are applied to your systems promptly**
   - When vendors release updates, hackers can determine how to break into systems that have not been updated.
   - Hackers then probe systems on the Internet looking for non-updated computers to attack.
   - Your system's software and application programs should be configured to apply or notify you of automatic updates when available.

3. **Confirm that up-to-date, anti-virus software is running on your systems**
   - Hundreds of new viruses are developed each day.
   - Anti-virus software can only detect and react to known viruses.
   - Your anti-virus software should be configured to automatically apply updates as frequently as possible, at least daily.
   - If you purchase your own anti-virus software for your personal system, remember to renew your subscription before it expires so that you continue to receive updates.

4. **Limit other systems' ability to access your computer with configuration settings, a firewall and other tools**
   - Configure wireless routers to only allow connections by authorized devices, e.g., require a key, password or registered MAC address.
   - Restrict network access to your system, especially on a public or home network, i.e., set up your system to not be discoverable, not share network folders and not accept remote desktop connections.
   - Windows, Mac, Linux and other systems have built-in firewall software that can stop computers from probing your system, and can block your computer, if infected, from attacking other systems.
   - A hardware firewall adds security by physically segregating the firewall functions from the system it is protecting.
   - Ensure the firewall you use is activated and configured to block unexpected network connections (in or out).
   - Adding a host intrusion prevention product can provide additional protection by blocking known attack patterns that it finds in the network traffic entering or exiting your system.

5. **Avoid doing every day work using an account with administrative privileges**
   - Set up your day-to-day account with user-level privileges.
   - If you inadvertently open a virus-infected application or link, it will only be able to perform functions on your system that your logged-in ID can perform.
   - Since user-level accounts typically cannot install software, viruses cannot be installed and executed on your system without your entering the administrator ID and password.
   - A second administrator level account can be used when you need to install software or to perform system administrative tasks.

6. **Lock any computer or mobile device left unattended**
   - Anyone who can access your logged-in system can do whatever you can do on your system without having to learn your password.
   - Timeout-based locks, i.e., locking the computer after a defined period of inactivity give an intruder too much time for mischief.
   - Manually locking your computer or mobile device prevents passersby from using your logged in session.
   - Avoid setting your system to automatically log into email and other applications that may hold personal data.

7. **Know the sensitivity of the data on your computers, mobile devices and storage media**
   - Information is considered sensitive if its exposure to unauthorized individuals would cause financial or reputational loss, including information that:
     - Can result in identity theft, such as social security numbers, account numbers, driver's license numbers, birth dates, passwords, etc.
     - Is protected by law or contract, or would pose any other risk to the University, if exposed.
   - Without understanding the sensitivity of the information held on your computer, mobile device or storage medium, you may inadvertently make sensitive information available to unauthorized individuals.

8. **Actively control access to sensitive data**
   - Make sure that, for any files and folders containing sensitive data, you indicate who specifically can access those files and folders and what they can do (e.g., read only, update, delete).
   - Beware of attempts to gain your confidence, and access to data, by individuals using "social engineering" techniques.
   - Always ensure that individuals to whom you give information are properly authorized.
   - Restrict what you share on social media sites. It could be used to steal your identity, be viewed by a prospective employer, etc.

9. **Ensure that your computers and mobile devices encrypt sensitive information when transmitting it over a network**
   - Unencrypted, sensitive data can be viewed when it travels across the Internet or is transmitted over an unsecured wireless network.
   - Virtual Private Network (VPN) technology improves security by encrypting all data passing between your computer or mobile device and the organization providing the VPN service.
   - When you send sensitive information to a web application, look for "https://" at the start of the web address and a lock icon displayed on your browser. It tells you that the traffic is encrypted.
   - Be careful when your browser shows that the identity of the target web site cannot be verified. It may be a counterfeit site.

Rev. 3 – Jan. 26, 2017

10. **Encrypt sensitive data on computers, mobile devices and storage media**
    - If you store sensitive information on your computer, mobile device or storage medium, encrypting your information reduces the risk of it being exposed if the device is lost or stolen.
    - Ask your IT support person or the OIT Help Desk at (609) 258-HELP for recommended products.

11. **Avoid using email to exchange or store sensitive information**
    - Messages originating from senders or destined for recipients outside of the University's email system, travel across networks and are stored on email systems managed by other organizations.
    - While the University is committed to following information security best practices for managing email, we cannot be certain that the same holds true for email and network providers outside of the University. So, you should assume that any email message sent to or received from an off-campus address is at risk.
    - If you must send or receive sensitive information via email, ask your IT support person or the OIT Help Desk at (609) 258-HELP for alternatives.

12. **Do not install any piece of computer software or mobile "app" until you have confirmed its security is effective**
    - Check with your IT support person or the OIT Help Desk at (609) 258-HELP to determine if the software has been approved for University use.
    - If the University has not reviewed the product, check the reviews published by well-known, respected product review organizations, such as C|NET, PC World, Mac World, etc.

13. **Protect your web browsing cookies**
    - "Cookies" are small files that websites send to your browser to facilitate your interaction with the site. If you've entered sensitive data into a website, it may be held in a cookie, but how well protected the cookies are is up to the website.
    - To ensure that one site does not obtain sensitive data by reading another site's cookies, set up your browser to delete all cookies when you exit, and make sure that, when you exchange sensitive information with a website, you close all browser windows before accessing another site.

14. **Use discretion when surfing the Web**
    - Avoid websites of organizations or individuals of an unknown or questionable reputation.
    - Shun websites that have a history of spreading malicious software, such as pop culture sites.
    - Before clicking a link, view the website's address by passing the cursor over the link (but not clicking). The website address that displays should point to a site name that you expect.

15. **Be discerning when clicking links or attachments**
    - Email messages can be made to look like they are from someone you know.
    - Before clicking attachments or links, be reasonably certain of the source, expect the attachment and know what the attachment contains.
    - Ask yourself, "Is this a note that my friend would send?" "Was I expecting anything like this?"

16. **Beware of the phishing threat**
    - Phishing is a scam that tricks you into providing passwords, social security numbers, bank account and credit card numbers, or other personal information while pretending to be from a legitimate institution.
    - ***Reputable organizations do not ask that you provide personal information in an email reply.***
    - If you receive a suspect message to your princeton.edu email, see if it has been reported to The Phish Bowl at informationsecurity.princeton.edu/phish-bowl. To submit suspicious emails to The Phish Bowl, delete any attachments and forward to phishbowl@princeton.edu.

17. **Be suspicious of unsolicited Web messages, warnings, popups and free services**
    - Responding to unsolicited messages, warnings and popups you receive while web browsing, especially ones promising free services, such as "We've detected a virus on your system!!" and "Click here for faster Internet!" may download malicious software onto your system or expose your Web traffic to unauthorized individuals, even if it is encrypted.
    - Avoid clicking anything on a popup window.
    - Close popups using your browser menu or system task bar.

18. **Wipe your computers, mobile devices and storage media before discarding, donating or repurposing them**
    - Deleting a file does not actually erase it. Systems delete files by marking the storage space the file occupies for reuse. Until that space is reused, the data is still there.
    - Disk shredding software erases individual files on demand.
    - Disk wiping software completely erases a storage medium.

PRINCETON UNIVERSITY

The Building Blocks Of Safe Computing

How to effectively protect information on the University's systems (and your own systems, too)

NOTE: If a University computer, mobile device, or storage medium is lost, stolen or compromised, or you suspect that sensitive University information has been exposed, please contact the OIT Help Desk immediately at (609) 258-HELP. Consultants are available 24 hours a day, seven days a week.

Information Security Office
Office of Information Technology

infosec@princeton.edu

Rev. 3 – Jan. 26, 2017