# UWM Research Data Stewardship

Whether a research project generates gigabytes or petabytes of data, proper stewardship is ultimately the responsibility of the project sponsor. UWM Information Security offers the following guidelines to help principal investigators (PIs) and information technology (IT) support personnel keep UWM research data safe.

For large-scale projects, professional IT support personnel salaries should be included in the project's budget. For self-managed projects, the sponsor can seek assistance from campus IT support personnel about system maintenance and proper data stewardship.

It's important to know which type of data is involved, and whether or not it's subject to specific laws or policies:

- The UWM Institutional Research Board (IRB) should be informed about research involving human subjects: https://www4.uwm.edu/usa/irb/.
- The UWM Legal Department will advise anyone dealing with data that is subject to HIPAA or other laws: https://www4.uwm.edu/legal/.
- UWM Libraries assists with the development of granting agency-required data management and sharing plans: http://uwm.edu/libraries/dataservices/
- For information about data classification, see the UWM Information Security web site: https://www4.uwm.edu/itsecurity/

# Top ten tips for keeping data safe:

1. **Practice safe Internet use.**

    a. Use OneDrive or PantherFILE to share files instead of sending or receiving attachments via email. Malicious individuals can spoof email and take control of your mailbox to send email attachments with malware designed to steal credentials or take control of your machine.
    b. Verify email message links before clicking on them. Email links can be used to lure you to sites that appear authentic where they request credentials or exploit web browser weaknesses to install software on your system that would allow someone else to take control of it.
    c. Only navigate to well-known (valid) websites. Navigating to unknown websites gives malicious people the opportunity to take control of your machine. If at all possible, use one machine for research purposes and another for email and web browsing.
    d. Password-protect all devices and auto-revert to the log on screen after two minutes of idle time.
    e. Use a firewall to block unwanted access.
        1. Windows - http://windows.microsoft.com/en-us/windows/understanding-security-safe-computing#1TC=windows-7
        2. Mac - http://support.apple.com/kb/ht1810

2. **Update operating systems and browsers as soon as new patches are released.**

    Most servers, workstations and laptops are directly exposed to the Internet which gives hackers an opportunity to scan them for weaknesses. By employing the automated update feature, systems are patched before malicious people can detect vulnerabilities.

a. Operating system (OS) auto-patching:

    1. Windows OS: Vista, 7, and 8: http://support.microsoft.com/kb/306525
       NOTE: Windows XP is no longer supported by UWM and will be blocked.
    2. Mac OS 10.7:
       https://answers.syr.edu/display/os/Automatic+Software+Updates+on+Snow+Leopard+and+Lion
       Mac OS 10.8:
       https://answers.syr.edu/display/os/Automatic+Software+Updates+on+Mac+OSX+Mountain+Lion
       Mac OS 10.9:
       https://answers.syr.edu/display/os/Automatic+Software+Updates+on+Mac+OSX+Mavericks

b. Web browser auto-patching:

    1. Internet Explorer: If auto-updates are turned on for the OS, IE should also be updated automatically. If not, make sure to turn them on in IE.
    2. Chrome: https://support.google.com/chrome/answer/95414?hl=en
    3. Firefox: https://support.mozilla.org/en-US/kb/advanced-settings-browsing-network-updates-encryption#w_update-tab

c. Java auto-patching:

    1. Mac OS X
        1. http://java.com/en/download/help/mac_java_update.xml
    2. Windows
        1. http://www.java.com/en/download/help/java_update.xml
        2. http://www.java.com/en/download/help/java_update.xml#manual

**3. Back-up data in a secure manner.**

a. Backing up to hard drives, USB Sticks, CD/DVD's, or other removable devices is not recommended since they can become lost, stolen, or damaged. Instead, store files on network drives that are backed up to off-site locations. If you are unsure, ask a local IT support technician for guidance.
b. Destroy obsolete media (old, unwanted back-ups) in an appropriate fashion. UWM Information Security can help with this process.
c. Encrypt data before it is backed up. If it is encrypted before being backed up, the data cannot be read while in transit or stored by individuals that should not be able to view it.
d. Educate administrative personnel during the on-boarding process, and on a continued basis about the importance of best practices associated with backing up business and research data.
e. Perform a risk assessment of your back-up process frequently.

4. **Use a dedicated research workstation.**

If possible, use one workstation exclusively for research, and keep a second machine for everything else. Or, create a second user name that doesn't have administrative rights on your workstation/laptop and use that account for day-to-day activities.

5. **Install and run only trusted applications.**

Never open email attachments from unknown senders (especially .zip, exe, bat, pdf, etc.). If

you aren't sure about an attachment or its sender, seek help from a professional IT support technician or the UWM Information Security Office.

6. **Encrypt computers, external hard drives, USB devices, and others that contain research data.**

   For assistance, ask a professional IT support technician or contact the UWM Information Security Office.

   a. Windows - http://windows.microsoft.com/en-us/windows-8/bitlocker-drive-encryption
   b. Mac - http://support.apple.com/kb/ht4790

7. **Use up-to-date anti-malware/anti-virus software.**

   Free antivirus software is available on the UWM Information Security website: http://www4.uwm.edu/itsecurity/tools/antivirus/index.cfm

   a. Make sure it's set to install daily updates (continuous scanning is better).
   b. Scan all media that's connected to the machine, including external hard drives, USB devices, and CD's.

8. **De-identify research data, if possible.**

   A separate, encrypted file with identifiable data can be retained, but use unique, nondescript keys in identifiable research data. See IRB's definition of identifiable data: https://pantherfile.uwm.edu/groups/sa/usa/irb/Website/Guidelines/De-identified%20Data%20Guidance%20August%202014.pdf

9. **Store encrypted research data on a shared network folder.**

   a. Most networked file servers are backed up on a regular basis and have other security controls in place, such as monitoring, logging file/folder access, access rights, and patching. Ask system administrators to verify the security controls.
   b. Files stored on workstations or external hard drives are often lost, or get corrupted.
   c. Never store identifiable data in the cloud. Cloud-enabled storage services, such as OneDrive, Google Drive or DropBox, do not have favorable terms or conditions for confidential or sensitive data. Once data is loaded onto these sites, it could be stored anywhere—it becomes their data. (OneDrive guarantees that it stores data in the U.S.). OneDrive security guidelines are available at: http://uwm.edu/o365/wp-content/uploads/sites/79/2014/07/OneDrive_Security_Recommendations.pdf

10. **Control access to data.**

    Grant physical and electronic access to data only to people who need it, and quickly remove privileges when that access is no longer needed.

Department IT support personnel are the first line of defense when it comes to protecting a department's systems and data. For additional guidance, contact the UWM Information Security office at infosec@uwm.edu or (414) 229-1100.