University of Washington IT Groups

Revised 6/14/2016

Setup and Use of UW Accounts (NetID, AMC, Outpost)

New faculty and staff set up their UW NetID password at the start of employment through UW IT services.

If your job function requires access to patient care-related data, a separate UW Medicine account will also be required for you.

UW IT Services: UW NetID

Phone: 206-221-5000
Email: help@uw.edu

UW NetID's are administered by UW Information Technology (UW-IT). A UW NetID is your personal identification for many UW online resources and applications. It is also required of everyone associated with the University of Washington who plans on using online central administrative programs and computing services. You will maintain this account throughout your life, even after you end your association with UW.

Example Usage:

- Access to the MyUW page (including Employee Self Service) from which you can check and/or modify your personal UW information. This includes employee payroll records, benefits files, your UW Directory information, etc.
    - MyUW Web Portal: https://my.uw.edu/
- Enable and access your UW email account, along with other computing services
    - @uw.edu/@u.washignton.edu email systems (UW Deskmail/Alpine, UW Exchange Online/Office 365)
- Access UW OneDrive for Business
- Access Catalyst surveys
- Update your UW Medicine (AMC) account password (if applicable)
- Log into the MedHub Residency Management System (if applicable)
- Access the UW Medicine Learning Gateway eLearning Modules (if applicable)

For First-Time Access:

If you are new to the UW then you need to get the PAC (Private Access Code) Code to get your NetID. The PAC was generated for you automatically in the payroll system and is provided to you by your Administrator or via email from the Finance Office.

1. Go to https://uwnetid.washington.edu/newid/
2. If you are new to the UW: Select the 3rd option - "I don't have a UW NetID (or I'm not sure)" – and then click on next or If you already have a NetID: Select the 2nd option - "I have a UW NetID but no password" – and then click on next
3. Select "UW Faculty, Staff, Retiree or Affiliate Employee" then follow the instructions from there on.

If you have difficulty establishing your UW NetID and password, please contact UW-IT for assistance.

UW Medicine IT Services: AMC Domain

Website: https://services.uwmedicine.org/
Phone: 206-543-7012
Email: mcsos@uw.edu
New user accounts, account changes and deactivations, audits: User Access Administration (UAA unit)

A UW Medicine (AMC) account is administered by the School of Medicine and enables access to UW Medicine applications. Your UW Medicine Account login name is the same as your UW NetID, but will have a different password.

Example Usage:

- Workstation support for AMC workstations (found in clinical areas)
- Access to ORCA PowerChart – UW Medicine inpatient Electronic Health Record (EHR)
- Access to EpicCare – UW Medicine outpatient EHR
- Access to MINDscape – Patient records for care received at UWMC, HMC, SCCA, UW Neighborhood clinics and outpatient records from NW Hospital Medical Center
- Access to UWCores – Web-based rounding and sign-out system to provide real-time data at patient bedside
- Access to Lapis or Hemingway file servers
- Access to websites that end in "uwmedicine.org"

These systems contain confidential patient information and should only be accessed by authorized personnel for official purposes. Security and confidentiality of information is required at all times.

For First-Time Access:

1. Go to MyUW: https://my.uw.edu/.
2. Click "Log in with your UW NetID".
3. Log-in with your UW NetID credentials (UW NetID & UW NetID Password).
4. Locate the "UW Medicine Computing Services" section and click "Change your UW Medicine password"

Department of Medicine IT Services (Outpost Domain)

Website: https://depts.washington.edu/domis
Phone: 206-616-8805
Email: ishelp@medicine.washington.edu
After-Hours Emergency Pager: 206-663-1597

Example Usage:

- Workstation support for Outpost workstations
- Access to Outpost Exchange email services
    - @medicine.washington.edu, @cardiology.washington.edu, @derm.washington.edu, @kri.washington.edu, @nephrology.washington.edu, @neurosurgery.washington.edu, @uwmedres.org, and @uwmedres.washington.edu addresses
    - https://mail.uwmed.org
- Access to personal Y drive and shared U drive for network file storage
- Remote Desktop access
    - https://depts.washington.edu/domis/remotedesktop

Password Change Website: http://depts.washington.edu/isalert/password/

Helpful Information

UW Email

Every person who has a UW NetID has a default email address of *your_uwnetid*@u.washington.edu and *your_uwnetid*@uw.edu. Both addresses will deliver to the same mailbox. Official UW messages for you will be sent to your default email address. If you are using another UW approved email address, you can set forwarding via the UW Email Forwarding page accessible through MyUW. More information about UW email is available at http://www.washington.edu/itconnect/connect/email/.
Approved domains that email can be forwarded to can be found on UW Medicine's website at https://depts.washington.edu/uwmedsec/restricted/resources/approved_email_domains/.

Data Stewardship: The most important things to know

Revised 6/14/2016

The ability to access information electronically provides convenience and enables productivity for all of us. Unfortunately, this convenience is also a risk. Don't be a victim of a data breach. Protect your equipment.

You are responsible for Data Stewardship

It is your responsibility to protect Confidential and Restricted information from being inappropriately revealed or damaged by anyone either maliciously or unintentionally.

- **Restricted Data** – data that is not regulated, but for business purposes, is considered protected either by contract or best practice (e.g. contract pricing, study data)
- **Confidential Data** – protection of confidential data is required by law
  - PHI (protected health information)–protected by HIPAA - All PHI breaches must be reported to the federal government Office for Civil Rights and to the State Attorney General, e.g. patient Information
  - Individual Student Records–protected by FERPA
  - Individual financial information (e.g., payment card, bank information)
  - Other personal information (e.g., Social Security number, home address, personal contact information, performance reviews)
  - Proprietary–intellectual property or trade secrets

Protect yourself from a breach of Restricted Data or Confidential Data

Assume your devices contain restricted or confidential data, even without intentional action on your part.

- Email can and often does contain some confidential or restricted information in attachments and in the body of long email threads
- Files that are synced from a file sharing system like *OneDrive for Business* may contain confidential or restricted information

Encrypt your devices – Never assume they are already encrypted

Encryption is not the same as Password protection. You need both!

Encryption protects the data storage units inside devices from being removed from the original device and read on another device. All of the following types of devices can be encrypted:

- Smart phones
- Laptops/Tablets
- Mobile devices of all types: thumb drives, jump drives, external hard drives, etc.
- Desktops (Encrypt desktops even if they are in a locked environment!)

Password protect your devices

Passwords help protect devices from access by anyone who is not authorized to do so.

- "Proper" passwords must be complex:
  - At least 8 characters in length
  - Contain at least 1 numeric character
  - Contain at least 1 symbol
  - Be a mix of upper and lower case letters
- Passwords should be changed often; at least every 120 days

<u>Password protecting and encrypting your computing devices greatly reduces the likelihood of a data breach in the event of a theft or loss!</u>

Free help with Password Protection, Encryption, and In-Place Computing:

If you are in the Department of Medicine visit a data Stewardship Kiosk

- To view the kiosk schedule: https://depts.washington.edu/domis/kioskschedule or call IS Help at 206-616-8805 to arrange an appointment or
- Email ishelp@medicine.washington.edu

Visit the DoM IT Services Web Site for more information:

- https://depts.washington.edu/domis

Visit the UW Medicine Security site for more information:

- https://depts.washington.edu/uwmedsec/

To find, lock, and/or remove data from your lost or stolen Cell Phone/Table:

- On Apple devices enable "find my iPhone/Mac" – Allows you to find and/or remotely remove data from your device.
- On Android devices use the 'Android Manager Website' – Allows you to find, lock, and/or remotely remove data from your device.

In-Place Computing: DO NOT copy information to your mobile or portable devices – if data is not on your device, a breach due to loss or theft cannot occur!

- Whenever possible use a web-based email application to access your email – this keeps your email on the server, not on your mobile/portable device!
    - If you use an email program e.g. Outlook, on your mobile device) the email is likely stored locally
    - If you use a program (e.g. Outlook) to access your email, configure it to not store (cache) email locally
- Use a VPN (virtual private network) to access UW Medicine resources from off the network
- Whenever possible use Remote Desktop or Terminal Server to work from off-site locations – this keeps the information off your mobile/remote device!
- If the UW system has an encrypted web interface (denoted by "https://"), use it instead of a desktop application – this keeps most information off your mobile/remote device!

Do not use unauthorized cloud or other offsite services

DO NOT send or store confidential or restricted information using unapproved cloud services or applications. The approved vendor products listed below are the only ones that may be used with confidential or restricted information, as the University of Washington has executed the appropriate legal agreements with the vendors for this purpose:

Cloud Applications Approved for use with Restricted or Confidential Information	Cloud Applications NOT Approved for use with Restricted or Confidential Information
OneDrive for Business	OneDrive
Skype for Business	Google Apps
Windows Azure	iCloud
Office 365	DropBox
	Amazon Web Services

For the most current information on cloud services visit:

https://depts.washington.edu/uwmedsec/restricted/guidance/cloud-computing/

Malware Infection Prevention: Don't let malware happen to you!

Revised 6/15/2016

There has been a tremendous increase in the number of malware attacks and they are getting more destructive and difficult to detect. Please familiarize yourself with the following tips and resources to protect your information at home and at work.

How devices infection occurs:

- Downloaded files from illegitimate websites.
- Opening unsolicited email attachments.
- Following links to infected/malicious websites.

All malware and viruses require disinfection of the device!

What you should do:

If you notice erratic behavior, a ransom request, or receive an alert from your antivirus on your device, shutdown your computer immediately!

If you have any questions or concerns, please contact the Department of Medicine IT for assistance:

- 206-616-8805
- ishelp@medicine.washington.edu

Malware types:

- Ransomware (Crytpolocker, Cryptowall, etc.):
    - Only use websites that belong to the actual company that you are interested in.
    - Never download a file from a site that is not associated to the company you are interested in.
    - Never open links or attachments in email that you are not expecting.
        - Do not run programs or open compressed (zip) files sent as attachments in email messages.
        - If you feel the email might be legitimate, access the site directly instead of using the link embedded in the email. If the email is not legitimate the link will direct to you a malicious website.
- Only connect to network shares/drives that you absolutely need access to.
- Disconnect from network drives when you are no longer accessing them.
- Make sure that antivirus is installed, enabled, and updated on all of your computers.
        - UW IT provides Sophos Antivirus at no cost. For more details, go to: http://www.washington.edu/itconnect/wares/uware/sophos-anti-virus-software/.
        - Microsoft provides Security Essentials for Windows Vista and 7 for free. For more details visit: http://windows.microsoft.com/en-us/windows/security-essentials-download/.
            - Windows 8 (and later) includes Windows Defender as the native built-in antivirus application.
- A sample screenshot of one of these ransomware programs:

- Spyware (Keyloggers):
    - Captures all the keystrokes on your keyboard and can relay this information to a third party facilitating in identity theft.
    - Keyloggers are extremely difficult to detect but pose a significant threat for identity theft.

- Make sure that antivirus is installed, enabled, and updated on all of your computers.
    - UW IT provides Sophos Antivirus at no cost. For more details, go to: http://www.washington.edu/itconnect/wares/uware/sophos-anti-virus-software/.
    - Microsoft provides Security Essentials for Windows Vista and 7 for free. For more details visit: http://windows.microsoft.com/en-us/windows/security-essentials-download/.
        - Windows 8 (and later) includes Windows Defender as the native built-in antivirus application.
- Adware (Conduit Search, Trovi Search Protect, etc.):
    - Adware highjacks search results and installs toolbars/extensions in your web browser.
    - Adware is not generally malicious in nature, but it can direct web traffic to malicious websites through illegitimate web search results.
    - Make sure that the popup blocker in your web browser is enabled.

Ways to protect your data:

- Store all your critical data on a server share that is incrementally backed up.
    - If you have a Department of Medicine IT Services full user account, then you have a mapped network drive assigned to you for this purpose with 35GB of storage. These network shares are incrementally backed up by IT Services and the helpdesk can restore this data for you to a date and time before an infection occurred.
- Use the University's free OneDrive for Business service.
    - This service supports versioning for files that are saved to the documents library and will allow you to recover files from different points in time, allowing the restoration of files to a point before an infection occurred.
        - See this link for more information: http://www.washington.edu/itconnect/wares/online-storage/onedrive/.

The Email Phishing Threat – Don't Get Hooked

Revised 6/15/2016

There has been a tremendous increase in the number of Email Phishing attempts and they are getting more malicious all the time. Please familiarize yourself with the following tips and resources to protect your information at home and at work.

Phishing Attempts are emails designed to trick you into giving up your personal and professional credentials, account information, and other identity information with the intent of stealing your identity, accessing your financial accounts to steal from you, and/or accessing professional information and systems you have access to in an attempt to steal or damage data.

If you have any question regarding an email you receive please contact the Department of Medicine IT Services for assistance:

- Phone: 206-616-8805
- Email: ishelp@medicine.washington.edu

What to do and not to do:

- NEVER open an attachment from an unknown source.
- If the context of the message doesn't make sense, delete the message or call the sender to verify the email.
- Always be wary of messages that ask you to update your password or confirm your account.
    - This can be tricky, because both the Department of Medicine and AMC IT Services notification of password expirations provide a link for you to use to update your password.
- Report any warning messages from antivirus or other software immediately to the Department of Medicine IT Services. Some malicious websites or popups say the computer has a virus, however the links provided are either malicious or a phishing attempt. DO NOT CLICK ON THE LINKS!
- Minimize the confidential information you store directly on your device.
    - Use network storage or UW OneDrive for Business whenever possible.
- Encrypt the data and your devices.
    - The Department of Medicine IT Services can provide assistance and advice for properly securing personal or work devices.
- Keep your operating system and software up to date (stay patched).
- Empty your email "trash bin" (Deleted Items) regularly or set the retention policy to purge after a certain timeframe or automatically when you exit your e-mail client application.
    - Doing so helps by getting rid of email messages that are no longer of use which may contain PHI and other restrictive or confidential data.
- Contact the Department of Medicine IT Services for assistance with any devices you use for work, both personal and UW owned. For Department of Medicine workforce members, assistance with device security is provided free of charge.

Educational Tools:

- UW Medicine IT Security Phishing Awareness Announcement: https://depts.washington.edu/uwmedsec/restricted/guidance/phishing-and-spam-email- guidance/
- Office of the Chief Information Security Officer phishing video: http://ciso.washington.edu/site/files/Phishing/story.html

Device Encryption Flowchart

Department of Medicine IT Services

Revised 6/14/2016