University Information Technology Services Northwest (UITS-NW), your connection to IT@IU. Below is a list of IT information and resources UITS-NW provide:

1. Media disposal
2. Software Packages Available
3. “23” Video Bridge Conference
4. File Storage
5. Patching and Maintenance
6. Loaner Equipment Program
7. Alertus
8. Secure Scans for Sensitive Data
9. Spam and Phishing Emails
10. Digital Signature
11. IU Fax Service

**Media Disposals**

UITS Northwest now offers the collection and disposal of electronic media. This service was implemented to give you the opportunity to dispose of media containing university data properly and securely. A secure locked bin is located in the UITS-NW Support Center where items can be dropped off during open hours. Physical storage media is then removed and handled by UITS staff in accordance with policy IT-12.

Items accepted include: flash drives, CD/DVD/BLUERAY disks, floppy/zip disks. **Please note:** You may dispose of any cases, wrappings, manuals, etc. yourself.

**Software Packages Available**

Software Packages are available for download (Software Center for PC and Self-Service for Mac)

As UITS Northwest deploys new lifecycle machines, users now have the ability to install select software packages on their own. No special login or Admin rights are required to install these software packages. You can view and install applications that are available via the following methods:

- The **“Self Service”** application on Mac systems, which can be found in the application folder
- The **“Software Center”** application on Window systems, which can be found by using the search option and typing in “Software Center”
**“23” video bridge conference**

IU offers no-cost virtual rooms for faculty, staff, and guests to meet online - at any time, from anywhere through “23” video bridge. “23” is a videoconference meeting service on the IU video bridge that allows users to meet and collaborate from web browsers, videoconferencing room systems, tablets, and smartphones.

Any IU faculty or staff member can create their own “23” VMR using the automated form at https://www.indiana.edu/~video/pexip/. Once created, your 23 conference is permanent and ready to receive calls anytime. The host controls access to the conference with an extra host PIN.

Every "23" video bridge conference has two aliases: a conference number, and a conference name. To connect to your conference, enter either 23<4-to-7-digit-number> or meet.name.

For connection instructions, see At IU, how can I create or join a videoconference?

*View a short video on "23" video bridge conferences.*

**File Storage**

At Indiana University, UITS provides a variety of baseline (i.e., no-cost) services for students, faculty, and staff needing to store, share, and collaborate on files. Some of these services are suitable for storing sensitive institutional data, and some are not.

- **Box at IU** provides a simple, secure way to share and store files and share folders online. You can create files and folders, share them using a direct link, invite others to collaborate, and continue to revise and review your content.

- **Canvas** provides online storage and file sharing for individuals, courses, and groups. In course and group spaces, files uploaded as attachments or assignment submissions are placed in the personal file space of the individual who uploaded them. Individuals also may upload files directly to their personal file spaces.

- **OnBase** is an electronic document management system used to store documents images and files on a central server. OnBase allows for the scanning, storage, and retrieval of paper documents, as well as the importing, storage, and retrieval of electronic files. OnBase is approved for storage of university critical data.

- **Slashtmp** provides a temporary way to share data with others via a web interface. It is particularly useful for sharing files that are too large to send via email. Slashtmp files disappear automatically 30 days after you upload them and files are not backed up.

If you work with institutional data at IU, you are responsible for meeting the university's official data management standards to prevent the inappropriate disclosure of personal or confidential information. Always follow best practices when storing sensitive institutional data; for example:

- **Never** store sensitive institutional data on your desktop workstation, laptop, USB flash drive, tablet, smartphone, or other mobile device unless the information is properly encrypted on the device, and your senior executive officer or the IU Institutional Review Board (IRB) has given prior written approval.

- **Never** store institutional data on removable storage media unless your senior executive officer and has given prior written approval and the data are properly encrypted. NOTE: In most cases, removable storage media
(e.g., flash drives, CDs, or DVDs) are appropriate only for storing personal, non-confidential files.

- **Never** store sensitive institutional data on an email or online storage system that is not part of the IU information technology environment.
  For details, see Standards for Management of Institutional Data.

### Patching and maintenance

UITS-NW utilizes an enterprise process to apply updates and patches to university owned desktop and laptop systems. We need your help to best ensure the safety and integrity of your university business and research data.

**Things to know and do:**

- At the end of every day, we ask that you leave your desktop system **logged off but powered on**; please **do not lock** the system when you leave for the day as this may interfere with needed security patch installations.

- UITS-NW has implemented a scheduled restart of all faculty/staff Windows computers every **Wednesday at 5:00am**. This schedule was implemented to complete the final step for the installation of Microsoft updates, and 3rd party updates (e.g., from Adobe, Apple, Java) to university Windows computers. Users will not be able to cancel the restart; you will receive a 1-minute warning before the scheduled reboot.

Thank you for your patience as we strive to provide a secure computing environment while minimizing interruptions to your work.

### Loaner Equipment Program

Thank you for continuing to make the UITS Northwest Equipment Loaner Program a huge success! This program provides equipment for faculty and staff for university related business. In order to make these resources available to as many people as possible, UITS Northwest has made some changes to the program.

- Equipment will only be loaned out to IU Northwest Faculty and Full-time Staff
- Equipment can be checked out for a maximum of 7 days within a 30-day period
- UITS Northwest Equipment Loaner Agreement must be signed before equipment is checked out
- Equipment may not be available during certain periods of time for maintenance purposes

Due to circumstances beyond our control, requested equipment may not be available. We will do our best to accommodate your request.

To request equipment for university business use, please fill out the [Equipment Request Form](https://iun.edu/technology) on the Information Technology Home page at [IUN.EDU/TECHNOLOGY](https://iun.edu/technology).

### Lectern technology in the classrooms
UIST-NW would like to remind all faculty, and especially new faculty, that staff are ready to assist you in classrooms for the start of the semester. A few points to help you as you use the technology in the classrooms:

- All classroom lecterns have a “Help Desk” button that allows an instructor to contact the UITS-NW Support Center for immediate assistance. Requesting assistance using the “Help Desk” button is the fastest way to get technology help when you are instructing a class!

- The first login on a lectern PC may take a minute or so as your profile is built. Please be patient; subsequent logins on that PC will be faster.

- Please remember to logout of the lectern PC before you leave a classroom; this will best ensure security of your data.

- The projectors take a minute to warm up and will shut down after 3 hours of inactivity as measured by activity on the lectern switch box. After the projector has shut down it will take 4-5 minutes to complete the shutdown process and turn back on again. If you would like to blank the screen, you may use the “Pic Mute” button.

**Alertus**

*Alertus* is used to distribute time-sensitive emergency notifications (fire, flood, active shooter, campus closings, etc...). Alertus desktop alerts are part of the [IU-Notify emergency notification system](https://www.iu.edu). Whenever IU-Notify issues an emergency alert, all workstations and laptops running the Alertus client will display a full-screen pop-up alert.

You can get more information at: Alertus pop-ups appear similar to the following:

[Alertus Alert](https://www.iu.edu)

**Emergency, Continuity & Planning**

*About emergency notifications at Indiana University*  
*What are Alertus desktop alerts?*
Secure Scans for Sensitive Data

**Is your computer protected?** Social security numbers are “critical” data and dates of birth or university ID numbers are “restricted” data and are not to be stored on individual workstations.

We have expanded our program to include desktop and laptop systems, in addition to home and departmental drives. **Identity Finder**, a self-monitoring tool that allows you to scan your university computer to detect whether you have critical or restricted data, has been deployed to all university owned computers.

Identity Finder is similar to a virus scanner, except it is looking for critical or restricted data on a hard drive instead of viruses. It can protect users from the consequences of potential data breaches of their computer files. Besides protecting the data of our student community, Identity Finder protects all of us. The laws governing identity theft may hold faculty and staff personally liable if their negligence exposes data. You can get more information on IU’s classification levels of institutional data by visiting [DATAMANAGEMENT.IU.EDU](http://DATAMANAGEMENT.IU.EDU) and selecting review data classifications.

Spam and phishing emails

If you use email, you’ve been on the receiving end of attempts to con you into giving up information or clicking on malicious links or files. These attempts have become increasingly sophisticated and are referred to as “phishing.” Scammers can create convincing emails that appear to come from trusted sources, including your bank or even IU personnel. These emails appear to look legitimate, but are actually a scam to entice you to click on a link to a fraudulent website that requests your IU credentials. Numerous IU employees have been deceived into revealing their IU passphrases in this manner. We see new phishing emails every week that sneak through IU’s spam filters (tens of thousands are blocked).

**Know how to avoid a fake.** Here are a few pointers from the University Information Policy Office (UIPO):

- It is very important to validate that the “from” address is actually the sender’s legitimate address.
- No one at IU should ask for your university passphrase or login credentials by email or over the phone.
- If you get an email or pop-up message that asks for personal or financial information, don’t reply — and don’t click on the link or call the number provided, either (instead use official contact details).
- Never email passphrases, personal, or financial information.
- Be cautious about opening any attachment or downloading any files from emails you receive, regardless of who sent them.
- Never click on a link in an email whose author you do not know.

**Remember:**

- No one at IU (including UITS) will ever ask for your passphrase, Social Security number, or confidential
personal information for any reason -- in person, via phone, chat, or email. Report phishing attacks to University Information Policy Office at PROTECT.IU.EDU.

- If you receive spam that appears to come from a valid IU account, UIPO will investigate.
- **Report** email breach, abuse, or spam to University Information Policy Office at PROTECT.IU.EDU.
- **DO NOT** click on any links or reply! Instead, simply right-click the message, choose “Junk,” and “Block Sender.”
- If you ever mistakenly share your passphrase, have clicked on a link inside of a phishing email or feel that your account has been compromised change your passphrase immediately. Go to ONE.IU.EDU and search passphrase reset.
- If you believe you’ve divulged confidential information as a result of a phishing scam, contact the University Information Policy Office.

For more information, visit:

- Phishing Education & Training [https://uits.iu.edu/phishing](https://uits.iu.edu/phishing)
- What should I do when I get spam email?
- What are phishing scams and how can I avoid them?

**Digital Signature: Is that email signed for?**

One way to help combat phishing attempts is to begin digitally signing emails that you send. Digital signatures certify that a message was sent from the account of the digital certificate holder, and was not modified during transmission. This provides the recipient a method of validating the actual sender of the email. Once a digital certificate is installed, emails are automatically signed in the background with no user action required. Your email recipients can verify your digital signature, and they can become accustomed to seeing the trusted ribbon next to your messages. If they know you always sign messages, they will be less likely to open unsigned messages from bad actors purporting to be you.

Digital signatures are supported in most email clients, including Outlook and mobile devices (Android and iOS). We encourage you to take advantage of this safeguard. There is no cost to you or to your unit to use this service; it is provisioned by UITS for the university.

Below are links that contain instructions on how to setup your digital signature. The process is two steps. You first need to obtain your certificate and then install it on each device you wish to send signed emails from.

**Step One:**

- Go to [KB.IU.EDU](http://www.kb.iu.edu) and search “digital signature (using S/MIME) at IU and following the instructions for obtaining a digital signature.” (Complete this before attempting to install using the below links)

**Step Two:**

- Go to [KB.IU.EDU](http://www.kb.iu.edu) and search the following instructions for installing a digitalsignature
• Using digital signatures for email with Microsoft Outlook for Windows
• Using digital signatures for email with Apple Mail and Outlook for OSX
• Using digital signatures for email on Android devices
• Using digital signatures for email on iOS devices

IU Fax Service

Need to send a fax? IU Fax is the Indiana University Fax Service that allows you to send faxes via a web interface. All IU Students, Faculty, and Staff who have a valid IU account can send a fax using the IU Fax Service by going to FAX.IU.EDU. (requires CAS authentication).

Need to receive a fax? Departments can contact the UITS-NW Support Center for assistance in establishing IU Fax to receive faxes for your department.

UITS-NW your connection to IT@IU!

UITS Northwest Hawthorn 108
iunhelp@iun.edu
http://www.iun.edu/technology
219-981-4357 (HELP)