# Department of Pathology Information Systems Guidelines

The Pathology Information Systems unit (PathIS) maintains all departmental servers, faculty and support staff computers, and peripherals. The department supports mainly Microsoft Operating Systems and Intel based computers for both workstations and servers and provides support for Macintosh Operating Systems.

Computers have their operating systems installed by the PathIS staff who will maintain the operating system's patches and fixes published by the software vendor(s). All software requiring any changes to the core Operating System (OS) will be evaluated and then installed by the PathIS staff after it has been determined that such changes do not interfere with UAB or Pathology usage and network policies. Software will be evaluated to determine any possible conflict with the operating system and security policies.

PathIS must maintain a complete inventory of all Departmental computers, including major computer related peripherals.

All departmental computers should be used in a professional manner in accordance with HIPAA regulations and the UAB Acceptable Use Policy, with the understanding that all computers belong to the Department of Pathology, UAB and the State of Alabama. As such, all computer related equipment/software should be used solely for UAB-related business.

The service level and security policies are different for different classes of computers within the department, which are detailed below in Section II. The categories are
Pathology Administrative staff computers, faculty computers, Research Laboratory computers and all computers that store and deal with protected Personal Health Information.

## I. Hardware and Software — Updates and Replacement Computer

## Systems Management

### Primary Faculty Office Computers

The department provides one computer for each faculty member. Systems will be provided with the most current Operating System (OS) available and current supported software (see "Current Software List installed on Pathology Computer", below). Secondary office computer will need to provide funds for PathIS to purchase the computer.
Each faculty member is potentially eligible for an upgrade on their primary computer after 3-4 years depending Path-IS assessment of individual needs and on the availability of sufficient departmental funds. The computer upgrade process is staggered. The computers being replaced are classified as "second-generation" computers and are distributed to research

laboratories, graduate and residents areas that need upgrading.

*The purchase of additional new computers and all computer peripherals must be reviewed and approved by PathIS prior to purchase to assure compatibility with its existing systems in order to be supported. This does not apply if PathIS is making the purchase.*

*Currently, PathIS does not have the resources to support PERSONAL owned computing devices or peripherals. Due to liabilities issues, PathIS highly discourages users bringing personal devices to UAB. PathIS cannot be liable for the loss of personal computing devices or peripherals.*

## UAB Laptops used for home remote

Each faculty is welcome to purchase a laptop or tablet to do work from home. This only applies to one (1) device per faculty. Peripheral purchased by PathIS for these devices can only be used on department own devices. Repairs for home laptops are low priority.

## Research Laboratories. Graduate and Resident Rooms

The department supports research laboratories of primary faculty. Computers and peripherals connected to the network will be provided using second generation systems as they are available, or by new computer equipment purchased by the faculty member using faculty UAB funds. Laboratory systems will be provided with the most current Operating System (OS) available and current supported software (see "Current Software List installed on Pathology Computer", on page 5). Users of research laboratory computers can be added at the request of the primary faculty member, independent of the user's primary departmental affiliation.
*The purchase of new computers and all computer peripherals must be reviewed and approval by PathIS prior to purchase to assure compatibility with its systems in order to be supported.*

## Software Licensing

The UAB guidelines for computer software use state that all machines on the UAB premises must have a legal copy of the software and abide by the manufacturers license. Therefore, correct and up-to-date licensing is important and it is illegal to use software that is not properly licensed. The department and/or individuals could be subject to fines for each instance where software is installed without a license.

The purchase of new software must be coordinated with the PathIS to assure compatibility with its systems and to avoid any HIPPA or other security issues. PathIS will keep the original licenses as they belong to the Institution.

File sharing (Kazaa, BearShare), server hacking, Trojans, illegal software and personal software are prohibited on the pathology network computer and pathology owned offline devices. These software/programs will be removed when found and the appropriate supervisor and faculty member will be informed.

## Data Security

### I. User Data Classifications

1. No access to ePHI
    a. Recommend using a timeout lock to prevent unauthorized use.
2. Access to ePHI using Pathology computer only as a terminal and no storage of data on the workstation or laptop.
    a. Recommend using a timeout lock to prevent unauthorized use.
3. Access to ePHI residing on a Pathology server.
    a. Require use of a timeout lock to prevent unauthorized access to ePHI data.
    b. Hard drive encryption of workstation might be required if the workstation is outside the Hospital network.
4. Access to and storage of ePHI on Pathology workstation or laptop computer.
    a. Hard disk drives and flash drives must be encrypted.
    b. Require use of a timeout lock to prevent unauthorized access to ePHI data.
5. Administrative Staff
    a. All administrative staff must save all work (completed or in progress) on Pathology servers at all times. Storage of work/files on hard drives or other devices is prohibited and can result in disciplinary action.

### II. **Automatic Lock**

As part of security and privacy it is recommended that computers are set to "lock" after a defined period of inactivity. A "lock" means the computer will require a password to continue operations. This prevents the following:

1. Unauthorized users or co-workers from using the computer to access private information found on the network.
2. Unauthorized users or co-workers from performing other illegal acts using another user's credential

This action is a MUST in case the assigned user leaves the workstation unattended and neglects to log off.

Access to applications containing ePHI, e.g., PathNet, Horizon, and Impact, is controlled by additional passwords and an automatic logoff occurs after a short time of inactivity.

### III. Encryption

All laptop computers used for UAB business must be encrypted to protect data from unauthorized disclosure. More Information: https://www.uab.edu/policies/Documents/PortableComputingDeviceSecurity.pdf

## Physical Security

Faculty members are strongly encouraged to provide sufficient physical security for their UAB owned computer equipment. A physical lock is highly recommended for laptop computers and they will be provided by the department, if requested. In addition, all laptops MUST be encrypted using Whole Disk Encryption which PathIS will provide upon loading new laptop or reloading existing laptops. Unless proper security measures are practiced, faculty and laboratory computers that are stolen must be replaced at the expense of the individual faculty member. Computers and portable storage devices that store ePHI require more intense review of physical security measures. All portable storage devices (PSD) that contain ePHI must be encrypted. See PSD Q&A at http://www.hipaa.uab.edu/pdffiles/Use_Portable_Devices_QA.pdf

## Authorized Users

An authorized user is anyone that can log onto the computer/network using a legitimate user name (BlazerID) and password. It is a violation of University, Health System and departmental policy to allow use of your logon by another individual regardless of their employment status. Failure to maintain security of passwords can result in disciplinary action.

Your user ID uniquely identifies you. It is your means for accessing a number of UAB/UABHS computer services. Other names for your user ID include BlazerID, Logon ID, and HorizonID.

- Do not share or allow anyone to use your user ID.
- Do not share or use another person’s user ID.

Protecting your password is critical in protecting confidential information. Follow these precautions:

- Memorize your password and never write it down.
- Change your password periodically.
- Do not share your password with anyone, including your supervisor and IT/HSIS representatives.
- Do not ask for or attempt to learn another person’s password.

Pathology IT (PathIS) representatives may ask that you login to a system for performing maintenance. Verify that they are authorized to perform the maintenance. Contact the appropriate Help Desk (PathIS, 4-6610) if you are unsure. Stay with the IT/HSIS representatives while they are logged into the system with your user ID and password.

You are responsible for all actions associated with your user ID and password.

## III. Process of Policy Review, Amendment, and Approval

Please send them to the Director of Information Services by email for consideration and approval.

## Appendix I – Approved default software

The following software is licensed to UAB and will be installed on all Intel/Microsoft OS based laboratory systems:

- Microsoft Windows 10 Enterprise
- Microsoft Office 2016 Professional Plus which includes:
  - Microsoft Excel
  - Microsoft PowerPoint
  - Microsoft Access
  - Microsoft Outlook
  - Microsoft Publisher
  - Microsoft Word.
- Adobe Acrobat Reader DC
- Adobe Acrobat DC (Faculty and Staff only)
- Adobe Flash Player
- Java
- Microsoft SCCM and Quest KACE (remote management, antivirus and patching)

For Apple OS, the installed software will include:

- Latest OS (as on early 2019, Mojave)
- Microsoft Office 2016
- Adobe Acrobat Reader
- Adobe Acrobat DC (Faculty and Staff only)
- Firefox Internet Browser (to access Oracle)
- Sophos Antivirus
- Microsoft SCCM and Quest KACE (remote management and patching)

## Appendix II – UAB Policies

HIPAA Policies: http://www.hipaa.uab.edu/index.php/policies.html

Other UAB IT related policies: https://www.uab.edu/it/home/it-related-policies