Department of Pathology Information Systems Guidelines

Owner: Department of Pathology Information Systems (PathIS)
Effective / Last Reviewed: May 2026
Review Cycle: At least annually, or sooner when UAB, UAB Medicine, HSIS, HIPAA, cybersecurity, or departmental requirements change.

1. Purpose

The Department of Pathology Information Systems unit (PathIS) provides information technology support for Department of Pathology computer systems, peripherals, departmental servers, approved software, and related technology resources. These guidelines define how departmental IT resources are requested, configured, supported, secured, used, and retired.

These departmental guidelines are intended to align with UAB, UAB Medicine, HSIS, HIPAA, Information Security, Acceptable Use, and data protection requirements. If a UAB, UAB Medicine, HSIS, HIPAA, or Information Security policy is more restrictive than this departmental guidance, the more restrictive requirement applies.

2. Scope

These guidelines apply to all Department of Pathology faculty, staff, trainees, residents, fellows, students, researchers, temporary workers, contractors, and other users who access or use Department of Pathology IT resources.

Covered resources include, but are not limited to:

- Department-owned desktops, laptops, Macs, tablets, and mobile devices.
- Departmental servers, virtual servers, storage, and shared systems.
- Printers, scanners, monitors, docking stations, and other peripherals.
- Department-supported software, licensed applications, and cloud-based services.
- Network-connected laboratory, research, administrative, and clinical workstations.
- Systems that access, process, transmit, or store UAB, UAB Medicine, departmental, research, business, confidential, restricted, or protected health information.

3. Ownership and Appropriate Use

All Department of Pathology computer equipment, software, peripherals, storage media, and related technology resources are the property of UAB, UAB Medicine, the Department of Pathology, and/or the State of Alabama, as applicable. These resources are provided for authorized UAB-related business, clinical, research, education, and administrative purposes.

Users are expected to use departmental IT resources professionally, securely, and in accordance with applicable UAB, UAB Medicine, HIPAA, Information Security, and Acceptable Use requirements. Users should have no expectation of personal ownership or privacy on UAB-owned equipment or systems, subject to applicable law and institutional policy.

4. PathIS Responsibilities

PathIS is responsible for supporting approved departmental IT resources, including:

- Installing and maintaining supported operating systems.
- Applying operating system, application, and security updates.
- Installing approved software and verifying software licensing.
- Maintaining an inventory of departmental computers and major peripherals.
- Coordinating endpoint security requirements with HSIS, UAB Information Security, and other institutional IT/security groups.
- Supporting departmental servers, shared systems, and approved storage locations.
- Coordinating computer replacement, redeployment, and return of equipment.
- Providing troubleshooting and escalation for supported departmental systems.

PathIS support is limited to approved UAB-owned or department-approved systems. Support for personally owned devices is limited and may be redirected to the appropriate UAB, HSIS, vendor, or external support channel.

5. Hardware Standards, Purchasing, and Replacement

PathIS must review and approve the purchase of new computers, printers, scanners, peripherals, and other network-connected equipment before purchase. This review helps confirm compatibility with departmental systems, institutional security requirements, warranty standards, network requirements, and supportability.

Faculty primary computers, administrative systems, laboratory systems, resident workstations, and shared workstations are replaced or redeployed based on business need, security requirements, system age, hardware condition, warranty status, available funding, and PathIS assessment.

Retired or replaced systems may be reimaged and redeployed when appropriate. A computer removed from one user or location may not be reassigned without PathIS review, inventory update, data review, and reconfiguration.

6. Operating Systems and Baseline Configuration

Departmental computers must run a supported operating system approved by PathIS and institutional IT/security requirements. Unsupported operating systems may be removed from the network, restricted, or replaced.

PathIS installs and maintains standard baseline configurations, which may include:

- Supported Microsoft Windows or macOS operating system.
- Required security tools and management agents.
- System encryption where required.
- Supported productivity software.
- Standard browsers and required plugins or runtimes where approved.
- Departmental shortcuts, printers, network mappings, or application access as needed.
- Inventory, patching, remote support, and endpoint management tools.

Users may not alter security settings, remove management agents, bypass endpoint controls, disable updates, or modify the operating system in a way that interferes with UAB, UAB Medicine, HSIS, Information Security, or PathIS requirements.

7. Software Installation and Licensing

All software installed on departmental computers must be properly licensed, approved, and compatible with institutional security requirements. Software that requires changes to the operating system, drivers, security settings, network configuration, or privileged access must be reviewed by PathIS before installation.

Users may not install unapproved, personally licensed, pirated, cracked, peer-to-peer, hacking, cryptocurrency mining, unauthorized remote access, or other prohibited software on departmental systems. PathIS may remove unapproved or unsafe software when

identified and may report the issue to the appropriate supervisor, faculty member, administrative leader, HSIS, UAB Information Security, or other institutional authority.

Software licenses purchased with UAB, grant, departmental, or institutional funds belong to the institution or department as applicable. PathIS may maintain license information or installation records as needed for compliance, support, and audit purposes.

8. Standard Software

The standard software installed on Department of Pathology computers changes over time based on institutional licensing, security requirements, operating system support, and departmental need. A current baseline may include items such as:

- Supported Microsoft Windows or macOS operating system.
- Microsoft 365 / Office applications, where licensed.
- Adobe Acrobat or Adobe Reader, where licensed and appropriate.
- Approved web browsers.
- Approved endpoint protection, monitoring, encryption, vulnerability, and management tools.
- Citrix or other approved clinical or enterprise access tools, when needed.
- OneDrive, UAB Box, network share access, or other approved storage tools, when appropriate.
- Department-approved printers, scanners, and related software.

Specialized software for research, clinical, administrative, educational, or laboratory use may be installed after review of license, compatibility, supportability, and security requirements. Some specialized software may require purchase approval, account number confirmation, vendor coordination, or renewal tracking.

9. Data Storage and Local Computer Storage

Departmental work files must be stored in approved UAB, UAB Medicine, or Department of Pathology storage locations. Approved locations may include departmental network shares, UAB-approved cloud storage, UAB Box, OneDrive for Business, approved departmental systems, or other institutionally approved repositories.

Files must not be stored only on the local computer, including the Desktop, Downloads folder, Documents folder, local C: drive, external drives, or other non-approved locations. Local storage is temporary and is not considered a supported or reliable storage location.

Local files may be lost due to hardware failure, profile corruption, malware remediation, operating system reload, computer replacement, security response, cleanup scripts, or other support activity.

PathIS cannot guarantee recovery of files stored locally. Users are responsible for saving work to approved storage locations. Administrative staff, clinical users, and users handling departmental business data must save work to approved storage locations at all times.

10. Confidential, Restricted, and Protected Health Information

Confidential, restricted, sensitive, regulated, or protected health information must be handled only in approved systems and storage locations. Users must follow all applicable UAB, UAB Medicine, HSIS, HIPAA, research compliance, data use agreement, and departmental requirements.

Electronic protected health information (ePHI) should not be stored locally on departmental workstations, laptops, desktops, removable media, or personally owned devices unless specifically approved and protected according to institutional requirements. Systems that access, process, transmit, or store ePHI may require additional safeguards, including encryption, endpoint monitoring, access controls, physical security review, and security approval.

Any suspected exposure, loss, theft, unauthorized access, or improper storage of confidential, restricted, or protected information must be reported promptly through the appropriate departmental, HSIS, UAB Information Security, privacy, compliance, or incident reporting process.

11. Portable Storage Devices and External Media

Use of flash drives, external hard drives, portable storage devices, or removable media is restricted and must comply with UAB, UAB Medicine, HSIS, HIPAA, and Information Security requirements.

Unencrypted or personally owned portable storage devices must not be used to store UAB business data, confidential information, restricted information, or ePHI. In clinical or hospital-managed areas, portable media may require HSIS review and approval. When portable storage is approved, it must meet institutional encryption and security requirements.

12. Passwords, Accounts, and Authorized Users

Users may only access systems using their own authorized credentials. Sharing user IDs, BlazerIDs, UABMC accounts, service accounts, passwords, badges, tokens, Duo access, or other authentication methods is prohibited.

Users must:

- Protect passwords and authentication methods.
- Use only accounts assigned to them.
- Never allow another person to use their account.
- Never ask for or use another person's account.
- Report suspected account compromise promptly.
- Follow institutional requirements for multifactor authentication, password changes, and account security.

PathIS, HSIS, UAB IT, and other authorized IT staff may ask a user to sign in when troubleshooting. Users remain responsible for activity performed under their credentials and should remain present when their account is being used for support unless otherwise directed by institutional support procedures.

13. Administrative Rights and Privileged Access

Local administrator rights are not permitted on standard Department of Pathology computers at this time. Users must not be granted standing local administrator access to departmental desktops, laptops, Macs, shared workstations, laboratory computers, or other supported endpoints unless a formal institutional exception has been reviewed and approved through the appropriate PathIS, departmental, HSIS, UAB Information Security, and/or Central UAB security process.

This restriction applies even when the user is the primary faculty member, principal investigator, supervisor, assigned user, device purchaser, grant owner, or primary operator of the computer. Purchase of a computer or software with departmental, grant, research, or other UAB funds does not create a right to local administrator access.

Local administrator access is restricted because it can allow users or software to bypass institutional security controls, install unapproved applications, disable endpoint protection, alter system configuration, interfere with vulnerability remediation, expose

confidential or regulated data, and create risk to UAB, UAB Medicine, the Department of Pathology, and connected systems.

At this time, PathIS will not approve routine local administrator access until additional security controls, privileged access tools, endpoint management capabilities, and/or institutional security solutions are available through UAB, UAB Medicine, HSIS, Central UAB Information Security, or another approved authority. Until those controls are in place, software installation, driver installation, configuration changes, troubleshooting, and other administrative actions must be performed by PathIS or another authorized IT/security group.

Users must not attempt to obtain, share, retain, bypass, escalate, or recreate local administrator access by any method. This includes using personal accounts, shared passwords, unauthorized local accounts, vendor-provided credentials, cached credentials, boot media, registry changes, scripts, remote access tools, privilege escalation tools, or any other workaround designed to bypass PathIS or institutional controls.

Vendor support, research equipment support, instrument support, software support, or time-sensitive operational need does not automatically authorize local administrator access. When elevated access is required for a supported business purpose, PathIS will coordinate the work directly with the user, vendor, faculty owner, departmental leadership, HSIS, UAB Information Security, or other institutional group as appropriate.

Any approved exception must be documented, time-limited when possible, tied to a specific business need, subject to review, and revocable at any time. Additional safeguards may be required, including enhanced monitoring, endpoint management, vulnerability scanning, encryption, logging, network restrictions, reimaging, or removal of the device from the standard network environment.

Unauthorized use or attempted use of administrative privileges may result in removal of access, reimaging of the computer, removal of unsupported software, network restriction, escalation to the user's supervisor or faculty owner, and referral to departmental leadership, HSIS, UAB Information Security, Compliance, or other institutional authorities as appropriate.

14. Security Updates, Endpoint Protection, and Network Availability

Departmental computers must remain available for security updates, vulnerability remediation, inventory, monitoring, and remote support. Users should not intentionally keep computers powered off, disconnected from the network, or blocked from management tools without a valid business reason.

PathIS may require systems to be powered on, connected to the appropriate network, or brought on site for updates, troubleshooting, installation, vulnerability remediation, or security review. Systems that do not check in, cannot be patched, or cannot be supported may be restricted, removed from service, reimaged, or escalated.

Users may not disable antivirus, endpoint detection, vulnerability scanning, encryption, firewall, device management, patching, logging, remote support, or other required security tools.

15. Physical Security and Device Protection

Users are responsible for reasonable physical protection of assigned equipment. Laptops, mobile devices, portable equipment, and small peripherals are especially vulnerable to loss or theft.

Users must:

- Secure laptops and portable equipment when unattended.
- Avoid leaving equipment visible in vehicles or unsecured locations.
- Report lost, stolen, damaged, or missing equipment immediately.
- Return equipment when no longer needed, when reassigned, upon separation, or upon request.
- Use approved encryption, tracking, management, and security controls as required.

UAB-owned equipment may not be taken outside approved work locations or outside the country without appropriate institutional review and approval. International travel with UAB-owned devices may require review by UAB, UAB Medicine, HSIS, UAB Information Security, Export Control, or other institutional offices.

16. Remote Access and Personally Owned Devices

Remote access to UAB, UAB Medicine, or Department of Pathology systems must use approved institutional methods. Unauthorized remote access tools, personal remote-control software, shared credentials, or bypass methods are prohibited.

Personally owned computers, phones, tablets, or storage devices are not managed by PathIS and may not be appropriate for accessing departmental, clinical, restricted, or regulated systems. When personal devices are permitted by institutional policy, users remain responsible for following UAB, UAB Medicine, HSIS, HIPAA, and Information Security requirements.

17. Research Laboratory, Resident, Graduate, and Shared Computers

Research laboratory, resident, graduate, and shared computers are supported based on departmental priority, security requirements, business need, available equipment, licensing, funding, and PathIS supportability.

Primary faculty members or designated owners are responsible for informing PathIS when users need access, when users no longer need access, when equipment changes location, when software needs change, or when a system is connected to specialized laboratory or research equipment.

Computers attached to laboratory instruments, research equipment, or specialized devices may require additional review before operating system upgrades, patching, software changes, or replacement.

18. Inventory, Reassignment, Return, and Disposal

PathIS must maintain inventory records for departmental computers and major peripherals. Users and supervisors must notify PathIS when equipment is moved, reassigned, replaced, damaged, lost, stolen, retired, or no longer needed.

Before a computer is reassigned, returned, disposed of, or redeployed, PathIS will determine whether data review, backup validation, secure wipe, reimage, inventory update, or security review is required. Users should not transfer computers directly between individuals or locations without PathIS involvement.

19. Exceptions

Exceptions to these guidelines must be reviewed and approved by PathIS and, when applicable, departmental leadership, HSIS, UAB Information Security, Compliance, Privacy, or other institutional authorities. Exceptions may be time-limited, documented, monitored, or revoked.

20. Policy Review, Amendment, and Approval

These guidelines should be reviewed at least annually by PathIS and relevant departmental leadership. Updates may also be made when institutional requirements, security standards, supported technologies, or departmental operations change.

Proposed amendments should be reviewed by PathIS and appropriate departmental administration. Final approval should follow the Department of Pathology’s applicable governance and approval process.

21. Contact PathIS

For Department of Pathology IT assistance, submit a PathIS ticket through the departmental ticket portal:

PathIS Help Desk: https://isp.path.uab.edu
Phone: 205-934-6610

For urgent security, privacy, HIPAA, or suspected data exposure concerns, users should also follow the applicable UAB, UAB Medicine, HSIS, Information Security, Compliance, or Privacy reporting process.