School of Dentistry Policy and Procedures for Acquisition of Computers, Software, and Devices

Effective Date: 01/07/2025

Policy Statement:

Requests for new computers and related information technologies in the School of Dentistry (SOD), including software, are made through the SOD Health Information and Business Systems (HIBS) ticketing system unless otherwise excepted below.

Rationale:

This policy and related procedures outline the acquisition of computers, devices, or software for the SOD. The intent is to ensure compliance with UAB Procurement process and UAB IT Technology Tool Governance process; entry in the SOD IT Inventory for service and support; configuration to access school and university resources; and integration into the University's IT infrastructure.

Scope:

This policy may include a wide range of devices used within the SOD and related clinics, including desktops, laptops, tablets, mobile devices, servers, network routers, switches, printers, scanners, and any other device capable of accessing or processing UAB data, or connected to networks associated within the UAB Enterprise.

Hardware in the IT Service Catalog are approved configurations for UAB use, otherwise, justification will be required for custom configurations. Smartphones or other devices requiring cellular network connectivity must be acquired directly through UAB Telecommunications and should be registered with HIBS if accessing SOD Systems (e.g., electronic health record).

Software, not currently approved as UAB Designated Technology Systems, may require a security governance review prior to acquisition, especially if using Sensitive Data, Restricted Data or Protected Health Information (PHI) as defined by the UAB Data Classification Rule.

Procedures:

1. **Initiating a Request:**
   - Users or department liaisons must submit a support ticket to HIBS at https://go.uab.edu/hibshelpdesk.
   - The ticket should include any specifications or special requests for the new computer or device.
2. **Requesting a Quote:**
   - HIBS staff will review the request to ensure the computer or device meets UAB IT and Procurement guidelines. If additional procedures, approvals, or security reviews are required, HIBS will initiate these processes (e.g., acquisitions requiring a BAA).

- HIBS staff will use the UAB IT Portal to request a quote for the desired Mac, PC, device, or software.

3. **Review and Ordering:**
   - Upon receiving the quote, HIBS will forward it to the department for review, user approval if applicable, and ordering.
   - Alternatively, if an account number is provided, HIBS staff can place the order on behalf of the department.
4. **Hardware Delivery and Setup:**
   - Upon arrival of the new computer or device, HIBS (or the department) will submit an AskIT request for the device to be delivered and set up for UAB business use.
   - This setup will include addition of UAB security, networking, and core applications. If the computer is to be managed and serviced under a UAB IT contract, this step is required.
5. **Software Installation:**
   - HIBS staff will work with the user to determine if any SOD-specific software (e.g., Salud, MiPACS, Citrix, SPM) needs to be installed.
6. **Inventory Registration:**
   - HIBS will register the new computer or device in the School Inventory for support, maintenance, and upgrades.
   - All computers and devices must be included in the inventory to effectively serve the School.

Compliance:
Compliance with this policy is required. Purchasing computers, devices, or software outside of this policy may lead denial of access to SOD or UAB systems as well as support from HIBS or AskIT.

Roles and Responsibilities:

- **Users/Department Liaisons**: Initiate requests and provide necessary specifications.
- **HIBS:** Request quotes, review requests, forward quotes, place orders (if account number provided), submit AskIT requests, assist with software installation, and register devices in the inventory.
- **Central IT:** Handle quoting, setting up devices, adding UAB security, networking, core applications, and ensuring compliance with UAB IT guidelines.
- **Health System Information Services (HSIS):** Handle security and compliance reviews for specific patient-related technologies and software.

Review and Updates:
This policy will be reviewed and updated yearly by the HIBS Manager and the Associate Dean of Clinical Affairs. If this School of Dentistry policy or procedures conflict with those of UAB Enterprise, university-level policies or procedures supersede in all cases.

Frequently Asked Questions (FAQ) for the
SOD Policy and Procedures for Acquisition of Computers, Software, and Devices

This FAQ is not policy and is provided for purposes of guidance and clarification. In all cases of a conflict of the following FAQ with this policy or any UAB polices, the policies supersede any guidance below.

1. **When buying equipment that includes a computer, device, or software, does it have to be reviewed by IT before ordering?**
   Many kinds of equipment (e.g., scanner, microscope, CBCT, etc.) have an associated computer, networkable device, or software specific to the equipment that may have configuration requirements by the manufacturer that differ from UAB. These systems need to be reviewed prior to acquisition, similar to all other technology acquisitions, for compatibility and compliance with UAB and SOD IT requirements.

   In circumstances where the computer, device or software conflicts with such requirements, HIBS and/or UAB IT will work with users and/or departments to mitigate such conflicts that include, but not limited to, security configurations, data management, or network considerations. Rarely, if unable to resolve and provide approved safeguards allowing use, then the computer, device, or software may not be allowable for use with UAB networks and/or data.

2. **What occurs in a security review?**
   Hardware and software technologies for UAB business use must be assessed for safety of UAB infrastructures, protection of data, and compliance with UAB policies as well as applicable state and federal law.

   For example, users often are required to accept a "Terms of Use" with new or upgraded systems or software, which frequently are in conflict with regulatory limitations of a public institution. Only specific administrators have authority to accept or sign on behalf of UAB (see Signature Authority FAQ), so "Terms of Use" must be reviewed prior to acquisition to avoid liability of an employee from inadvertently accepting terms on behalf of the institution. Another example regards contracts which must follow the UAB Procurement policies to adhere to regulatory requirements. Warranties often have a contractual relationship requiring review. Finally, any hardware or software using Sensitive or Restricted Data including HPI must have a review, which includes the vast majority of academic, research, and patient care data.

   The security review identifies these and other common considerations for the protection of the university, employees, students, and patients.

3. **Can I use a personally owned device with UAB or School of Dentistry systems?**

UAB strongly advocates that all university business activities be performed on UAB-owned computers and devices with appropriate security applied. Some systems will not allow a non-UAB device to connect. Nonetheless, the UAB Acceptable Use Policy allows personal devices for an employee's personal use at UAB, but adherence to all applicable IT policies are required. This includes appropriate safeguards such as firewalls, anti-malware software, password security, etc.

4. **Are student and resident-owned computers covered by this policy.**
This policy is not applicable to personally owned devices. Student and resident owned devices for academic access is allowed by the UAB Acceptable Use and related IT policies. This would include access to Canvas and other resources offered by the University. As determined by the School of Dentistry, student and resident-own computers and devices may be authorized for official patient-care activities such as connection to the electronic dental record. However, each device must be registered with HIBS where specific configurations are employed for security compliance. Failure of the student or resident to comply with these procedures may result in loss of privileges to access SOD resources and/or loss of clinical privileges.

HIBS Helps!!! Ordering a new computer or device