IOWA STATE UNIVERSITY
College of Liberal Arts and Sciences

LAS Information Technology

LAS IT Computer Requirements

The College of Liberal Arts and Sciences is committed to providing its faculty and staff with access to the computers, devices and storage that they need to fulfill our mission in teaching, research, and service to the best of their abilities. The college understands that information technology needs vary widely across our different departments, due to different teaching and research practices and needs. The college also appreciates that different research programs may have unique requirements.

Similarly, the college is committed to providing an information technology environment that meets the highest standards in terms of data security, privacy and accessibility. ISU is required to follow applicable federal and state laws. Hackers are sophisticated, and we need to ensure that all LAS faculty, staff and students understand the risks. Security breaches expose the university and the college to potentially significant legal and financial liabilities; they can severely impact the ability of others to perform their jobs. Faculty, staff and students also need to understand that they can be held personally liable if their actions are found to be in violation of ISU and LAS policies.

For these reasons, all faculty, staff and students in the College of Liberal Arts and Sciences are expected to follow the policies and practices outlined below. It is essential that they and their department chairs consult with ITS and LAS IT personnel with regards to any systems which store, process, or grant access to protected information.

- **Account credentials shall not be shared under any circumstances.**
- LAS IT personnel must be involved in the acquisition of all computers and data storage devices (e.g. servers, desktop computers, laptops, tablets, external hard drives, etc.) and any acquisition of software to be installed on these devices
- For the purposes of this document an ISU computer is defined as any electronic device that processes data associated with ISU activities, was purchased with ISU funds or is managed by ISU personnel. ISU funds include general fund dollars, grants and contracts, PI incentive funds, and donor support
- LAS IT personnel must be involved in the procurement of any cloud services or third party software or data services
- LAS IT personnel will implement an ongoing security audit of all computers (including servers, laptops, tablets, etc) purchased with ISU funds. The audits may scan for sensitive data including:
    - social security numbers,
    - credit card information,
    - user/password data, and
    - other personal information (e.g., university IDs, dates of birth, etc).
- LAS IT personnel will work with departmental and research group system administrators to analyze, purge, or securely archive data, in compliance with ISU data management policies. Standard encryption technology is required for all portable media.
- As data stewards all LAS faculty and staff will work with LAS IT to ensure the confidentiality, integrity and appropriate availability of all ISU data, according to the IT Security Plan https://security.it.iastate.edu/policies/it-security-plan and PI handbook https://www.vpresearch.iastate.edu/policies/)
- All employees should be familiar with and follow existing ISU policies on information technology security and electronic privacy (see, e.g., IT Security Policy, Electronic Privacy, Social Security Number Policy and Minimum Security Standards and Guidance found at https://www.policy.iastate.edu/policy/information-technology)

- LAS IT will coordinate training on IT Standards
- Faculty, staff, and students will also follow ISU data policies in relation to ISU data stored on personal devices. This includes not storing data with a classification above low on personal devices
- The LAS IT technician and their backup technician will have administrative access to all ISU computers (including servers, laptops, tablets, etc.)
- All ISU accounts must meet university security standards (authentication, etc.)
- Authenticated access and secure transmission of data will be required to access all non-public campus services from off-campus computers. Public campus services must be coordinated with LAS IT staff. Regular audits will be performed.
- Department chairs may request exceptions to any items in this policy by contacting Associate Dean Arne Hallam; exceptions will only be granted if security audits will be performed on a regular basis in close coordination with ITS and LAS IT personnel.

> You can download a PDF version of this document here: lasit-computer-requirements.pdf

Category: Support Documentation Standard Operating Procedures

Tags: procedure requirements management