

IOWA STATE UNIVERSITY

College of Liberal Arts and Sciences

Protection and Management of Digital Information

Guidelines on Purchase, Deployment, and Management of Information Technology Equipment and Software

Updated: 14 November 2025

Security breaches pose a severe risk to Iowa State University in terms of reputation and financial liability. They also pose a risk to employees/students. Insecure data and systems can lead to identity theft, data loss, phishing attacks, and potential financial liability.

Data security must take priority over personal convenience.

Iowa State University has developed a suite of data classification and information security policies posted at the [ISU Information Technology Policy Website](#).

All employees should familiarize themselves with and follow existing ISU policies on information technology security and electronic privacy:

[ISU Minimum Standards for Security](#)

[ISU Social Security Number Protection Policy](#)

[ISU Faculty and Staff FERPA Guidelines](#)

[ISU Electronic Privacy Policy](#)

[ISU IT Security Policy](#)

Data Classification Standards and Guidance

The college will implement and monitor the following security policies and practices.

1. LAS IT personnel will be involved in the purchase of all network-attached electronic devices (servers, desktop computers, laptops, tablets, external hard drives, and research equipment, or Internet of Things devices that connect to the internet, etc.) if these purchases involve ISU funds.
 - 1.1. ISU funds include grants, PI incentive accounts, and professional development funds.
 - 1.2. LAS IT personnel will also be involved in purchasing and installing all

software to ensure it meets ISU data security requirements and any licensing restrictions.

2. LAS IT personnel will perform ongoing security audits of all computers (including servers, laptops, desktops, and tablets) purchased with ISU funds.
 - 2.1. LAS IT personnel will work with departmental and research group system administrators to analyze, purge, or securely archive such data in compliance with ISU data management policies.
 - 2.2. The audits will be performed using identity detection software which scans systems for sensitive data including:
 - 2.2.1. Social Security Numbers
 - 2.2.2. Credit Card Information
 - 2.2.3. Authentication Credentials (e.g., usernames, passwords)
 - 2.2.4. Other personal information (e.g., University IDs, dates of birth)
3. LAS IT technicians assigned to your area will have administrative access to all computers (e.g., including servers, laptops, tablets) purchased with ISU funds. This is the most effective way of ensuring appropriate data management.
 - 3.1. To ensure the application of security patches, system encryption, and malware protection, systems will be registered and managed through campus information systems (e.g., JAMF, MECM, AD, MBAM).
 - 3.2. Department chairs may request exceptions by contacting Associate Dean Arne Hallam.
 - 3.2.1. Exceptions will only be granted on a limited basis and with a well-defined need.
 - 3.2.2. Exception systems will require regular security audits performed in close coordination with ITS and LAS IT personnel.
 - 3.2.3. ITS and LAS IT personnel must be consulted concerning any systems that store, process, or grant access to protected information.
4. Computers, by default, will not be configured to give administrative access to users.
 - 4.1. Software required for daily work is already pre-installed and configured or can be accessed through Software Center on PCs or Self Service on Macs.
 - 4.2. This approach helps maintain system security, stability, and compliance with organizational standards by preventing unauthorized changes or installations that could introduce vulnerabilities.
 - 4.3. Any software that is not already available or not on the list of approved software must go through a review process to ensure they meet business needs, comply with licensing and security policies, and do not conflict with existing systems.
 - 4.3.1. Please use the Software Review Request form for all new software requests: [Software Review Request Form](#)

5. External hard drives or additional local storage (amounting to making a computer server-like) must be approved by IT prior to use due to security, compliance, and data management concerns.
 - 5.1. These devices can potentially bypass centralized monitoring and backup systems, increasing the risk of data loss, unauthorized access, or data breaches.
 - 5.2. Storing sensitive university information outside approved infrastructure may also violate regulatory or legal requirements.
 - 5.3. To ensure proper protection, auditing, and support, all local storage solutions must receive formal approval from IT.

6. Servers at ISU are required to operate in the Durham 0095 Datacenter provided by ITS. To initiate the setting up of a server at ISU, please work directly with your LAS IT representative or a member of the ITS Research IT team. An exception may be granted after a careful review process involving ITS and LAS Administration.
 - 6.1. A server is any device or system—physical, virtual, containerized, or embedded—that provides shared services, data, or computational resources to one or more clients over a network.
 - 6.2. Classification is based upon the system’s function and intended use, not on its hardware or operating system. Examples include websites, applications, databases, files, proxies, and print servers, as well as virtual machine hosts or other devices providing service-oriented functions.
 - 6.3. Typically, systems are considered servers if they meet one or more of the following criteria:
 - 6.3.1. They host or deliver services accessible to multiple users or devices.
 - 6.3.2. They operate continuously or unattended.
 - 6.3.3. They provide centralized resources or management to other systems.
 - 6.4. ITS and LAS Administration will make the ultimate decision on whether a system meets the criteria of a ‘server.’

7. University personnel interact with all types of information. Various controls are required, depending on the sensitivity of the information. Direct all questions about which controls to apply to your local IT technician.

8. IT personnel will report all IT security incidents immediately to the ISU IT Security (security@iastate.edu) and to LAS IT Security (las-security@iastate.edu).