IOWA STATE UNIVERSITY
OF SCIENCE AND TECHNOLOGY

College of Liberal Arts and Sciences
Office of the Dean
202 Catt Hall
Ames, Iowa 50011-1301
515 294-3220
FAX 515 294-1303

Interoffice Communication

DATE: September 20, 2023

TO: LAS Faculty and Staff

FROM: Beate Schmittmann, Dean, College of Liberal Arts & Sciences

SUBJECT: Protection and Management of Digital Information

Security breaches pose a severe risk to Iowa State University in terms of reputation and financial liability. They also pose a risk to employees or students: If your data are exposed, you might become the victim of identity theft and incur financial losses. It is on all of us to work together to keep institutional and personal data secure. **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 Policy Library website: https://www.policy.iastate.edu/policy/dataclassstdguid. It is a college priority to implement and monitor these security policies and practices.

I am writing to remind you that, several years ago, LAS instituted the following steps to ensure that we are the campus leader in data management and information security. These steps were important then, and are even more important today:

1) LAS IT personnel will be involved in the purchase of all network-attached electronic devices (servers, desktop computers, laptops, tablets, tablets, external hard drives, and research equipment, or Internet of Things devices that connect to the internet, etc.) if these purchases involve ISU funds. ISU funds include grants, PI incentive accounts, and professional development funds. 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 perform ongoing security audits of all computers (including servers, laptops, tablets, etc.) purchased with ISU funds. The audits will be performed using identity detection software which scans for sensitive data including:
    - social security numbers
    - credit card information
    - authentication credentials (user/password)
    - 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 such data in compliance with ISU data management policies.

3) LAS IT technicians assigned to your area will have administrative access to all computers (including servers, laptops, tablets, etc.) purchased with ISU funds. This is the most effective way of ensuring appropriate data management. In order to ensure the application of security patches, system encryption, and malware protection, systems will be registered and managed through campus information systems (JAMF, MECM, AD, MBAM, etc.)

   Department chairs can request exceptions by contacting Associate Dean Arne Hallam. Exceptions will only be granted on a limited basis and with a well-defined need. Exception systems will require regular security audits performed in close coordination with ITS and LAS IT personnel. You must consult with ITS and LAS IT personnel concerning any systems that store, process, or grant access to protected information.

4) Email "phishing" has become a frequent, ongoing issue. Emails that appear to be from the department chair, dean, or staff asking for immediate cash transfers (gift cards), passwords, or security codes are almost always scams. IT will never ask for a password or an MFA code over email or SMS. Keep alert and if you have any concerns about whether an email is legitimate or not, contact your local IT technician.

5) University personnel interact with many types of information. Depending on the sensitivity of the information, various controls are required. Everyone should be familiar with the minimum security standards (https://www.policy.iastate.edu/policy/minsecstdguid). Questions about which controls apply can be directed to your local IT technician.

6) All employees should also be familiar with and follow existing ISU policies on information technology security and electronic privacy:
   - https://www.policy.iastate.edu/policy/it/security
   - https://www.policy.iastate.edu/electronicprivacy
   - https://www.policy.iastate.edu/policy/ssn
   - https://www.registrar.iastate.edu/resources/policies/ferpa-need-to-know

Let me stress that IT personnel are required to report all IT security incidents immediately to the ISU IT Security (security@iastate.edu) and the LAS IT Security (las-security@iastate.edu) teams.

We are committed to keeping our student, faculty, and staff information – including yours! – protected against any unauthorized intrusions.

Thank you for working with your IT personnel to safeguard our data.

With best wishes,

Beate Schmittmann, Dean

Beate