Electronic Privacy

Effective: November 8, 2012
Contact: Information Technology Services (ITS)

Contents

Introduction
Policy Statement
1. Privacy and Confidentiality
2. Exceptions to Privacy of Information
2.1 State and Federal Law
2.2 Proxy Access to Accounts Necessary to Conduct Business or Research
2.3 Investigations
2.4 Official University Business
2.5 Internal Administrative Disclosure
2.6 Maintenance of Iowa State University Network and Systems
2.7 Legal Disclosure Requests
2.8 Health and Safety Emergency
2.9 Authorization
Resources

Introduction

Iowa State University is required by federal and state laws to keep certain information confidential. Privacy and confidentiality must be balanced with the need for the university to manage and maintain networks and systems against improper use and misconduct.

Policy Statement

1. Privacy and Confidentiality

To the extent permitted by law and university policy, Iowa State university maintains and protects both the privacy of individuals and the confidentiality of official information stored on its information technology (IT) systems. While the university permits limited incidental use of its IT resources, users of those resources do not acquire an expectation of privacy in communications transmitted or stored on university information technology resources. In order to comply with the law, university officials may have direct access to stored information as described below.
top

2. Exceptions to Privacy of Information

Data traversing or stored in university systems are subject to disclosure requests under public records law, under subpoena, and in the discovery process in litigation. Iowa State University may preserve, access, monitor, or disclose information containing all classes of data as described in the **Data Classification policy** *(policy is pending; see Resources below)* residing on its information networks and systems in the following situations:

2.1 State and Federal Law

All information including the personal, academic, or research data and files residing on university systems is subject to state and federal laws and regulations requiring its disclosure, including laws on public records, court-ordered disclosure, and discovery in litigation.

2.2 Proxy Access to Accounts Necessary to Conduct Business or Research

Faculty and staff may need access to accounts of other faculty and staff when that individual is not available but access is needed to conduct university business or further research. Approval to access the account should be given either by prior proxy access to the individual's account or by written recommendation and justification by the individual's department chair or director and approval by a senior vice president or the senior vice president and provost or other designee acting on the basis of university policy and law.

2.3 Investigations

Iowa State University may preserve, access, or monitor accounts and equipment during the course of an investigation of misconduct, violations of law, or violations of university policy by students or employees. Access must be approved in writing by the senior vice president for business and finance, senior vice president and provost, or other designee acting on the basis of university policy and law. In accessing the account or equipment, university officials are expected to avoid accessing

information that is personal and irrelevant to the investigation.
top

2.4 Official University Business

As part of their assigned responsibilities, Iowa State University faculty and staff may have access to all classes of data and are restricted to using it only for purposes associated with the requirements of their position.

2.5 Internal Administrative Disclosure

Disclosure or use of any information containing data with a high or moderate security category for extraordinary circumstances must be approved in writing by the senior vice president for business and finance, senior vice president and provost, or other designee acting on the basis of university policy and law.

2.6 Maintenance of Iowa State University Network and Systems

Iowa State University reserves the right to maintain its information systems; to audit networks and systems on a periodic basis to ensure compliance with security policies; and to locate and resolve security breaches or other situations that potentially impact the reliability, robustness, or security of the campus network and systems infrastructure. Individuals performing these functions or others may have access to information containing all classes of data and are restricted to using it only for purposes associated with their position.
top

2.7 Legal Disclosure Requests

Iowa State University may preserve, access, and disclose information contained in its IT systems in response to a lawfully issued records request, subpoena, court order, or other compulsory legal process (“disclosure request”). To the extent possible and practical, the account holders for email and electronic files will be notified in advance of access or disclosure.

The public records officer, the research integrity officer or an attorney in the Office of University Counsel may order preservation of electronic records to comply with a disclosure request or to preserve records for purposes that may relate to pending investigations or litigation.

Access to email and electronic files must first be approved by the senior vice president for business and finance, senior vice president and provost, or the president. upon approval, attorneys in the Office of University Counsel may request or conduct targeted searches of electronic files to find material relevant to the disclosure request. In accessing the files, attorneys shall limit access to material that is relevant to the disclosure request.

2.8 Health and Safety Emergency

In the event of a health or safety emergency, Iowa State University may preserve, access, or disclose information containing all classes of data necessary and relevant to addressing the emergency situation.

2.9 Authorization

Iowa State University may preserve, access, or disclose information containing all classes of data relating to an individual student or employee upon the written authorization of the individual student or employee.
top

Resources

Links

- Acceptable Use of Information Technology Resources policy
- Information Technology Security policy
- Information Technology Policies and Procedures
- Office of University Counsel
- Public Records Officer Pam Cain
- Research Integrity Officer Wolfgang Kliemann
- Data Classification policy (DRAFT)

Files

- Electronic Privacy [Policy in PDF with line numbers]