IT Security

Effective: July 1, 2004
Updated/Revised: November 8, 2012
Contact: Information Technology Services (ITS)

Contents

Introduction

Iowa State University acknowledges its obligation to ensure appropriate security for information and IT (information technology) systems in its domain of ownership and control. Furthermore, the university recognizes its responsibility to promote security awareness among the members of the Iowa State University community.

Iowa State University develops, publishes, and enforces policies and standards in order to achieve and maintain appropriate protection of university information and information processing systems. This document along with related information security policies and standards (see Resources below) identifies key security issues for which individuals, colleges, departments, and units are responsible.

1. Policy Statement

Every member of the university community is responsible for protecting the security of university information and information systems by adhering to the objectives and requirements stated within published university policies. Also, individuals are required to comply with the additional security policies, procedures, and practices established by colleges, departments or other units. If multiple policy statements or security standards are relevant for a specific situation, the most restrictive security standards will apply.

Failure to comply with established policies and practices may result in loss of computing privileges and/or disciplinary action.

All units—from the university level through the college, department, and unit level—must provide opportunities for individuals to learn about their roles in creating a secure IT environment.

2. Specific Roles and Responsibilities

2.1 Chief Information Officer (CIO)

The Office of the Chief Information Officer has overall responsibility for the security of the university's information technologies. Implementation of security policies is delegated throughout the university to various university services (noted below); to colleges, departments, and other units; and to individual users of campus IT resources.

2.2 Data Steward

The data steward is the university office represented by an executive officer charged with the primary responsibility and authority to ensure that Iowa State University meets external and internal requirements for privacy and security of specific types of confidential and business data owned by the university in their functional areas. These data stewards, as a group, are responsible for recommending policies, establishing standards and guidelines for university-wide data administration activities. Data stewards may delegate the implementation of university policies, standards, and guidelines to data custodians. They are also responsible for advising colleges, departments, units, and individuals in security practices relating to these areas:

- Financial information and transactions (Treasurer's Office)
- Health information (Director, Thielen Student Health Center)
- Infrastructure, communications, and systems security (Information Technology Services)
- Law enforcement information (Iowa State University Police)
- Legal issues (Office of University Counsel)
- Library circulation records (Iowa State University Library)
- Personnel information and confidentiality (University Human Resources)
- Physical building security (Facilities Planning and Management)
- Regulated material information (Environmental Health and Safety)
- Research data and sponsored programs information (Vice President for Research)
- Security audits (Office of Internal Audit)
- Student loan information (Office of Student Financial Aid)
- Student record information and confidentiality (Office of the Registrar)

2.3 Data Custodian

The data custodian is the individual or entity (including outsourced services) in possession or control of data and is responsible for safeguarding the data according to the policies and procedures established by the associated data steward. The appropriate level of protection is based on the **Data Classification policy** and the **Minimum Security Standards for Protected Data** *(see Resources below)*.

2.4 Data User

The data user, synonymous with user, is the individual, automated application or process that is authorized by the data steward to create, enter, edit, and access data, in accordance with the data steward's policies and procedures. Users have a responsibility to:

- maintain the security of passwords, personal identification numbers (PINs), authentication tokens and certificates; and will be held accountable for any activities linked to their accounts
- manage all forms of authentication and security controls to information processing systems based on the Minimum Security Standards for Protected Data

- use the data only for the purpose specified by the data steward
- comply with controls established by the data steward
- prevent disclosure of confidential or sensitive data
- report suspected security incidents that may have breached the confidentiality of data

2.5 Colleges, Departments, and Other Units

Colleges, departments, and other units are responsible for securing any information they create, manage, or store, and for any information they acquire or access from other university systems (e.g., student educational records, personnel records, business information). This responsibility includes completing periodic risk assessments, developing and implementing appropriate security practices, and complying with all aspects of this policy.

2.6 Individuals Using Personally-Owned Computers and Other Network Devices

Students, faculty, and staff who use personally-owned systems to access university resources are responsible for the security of their personally-owned computers or other network devices and are subject to the following:

- The provisions of the IT Security policy and the standards, procedures, and guidelines established by IT Services for university computing and network facilities.
- All other laws, regulations, or policies directed at the individual user.

2.7 Third Party Vendors

Third party vendors providing hosted services and vendors providing support, whether on campus or from a remote location, are subject to Iowa State University security policies and will be required to acknowledge this in the contractual agreements. The vendors are subject to the same auditing and risk assessment requirements as colleges, departments, and other units. All contracts, audits and risk assessments involving third party vendors will be reviewed and approved by the university data steward based on their area of responsibility.

2.8 Other Registered Entities

Any entity that is a registered user and connected to the university network is responsible for the security of its computers and network devices and is subject to the following:

- The provisions of the IT Security policy and the standards, procedures, and guidelines established by IT Services for university computing and network facilities.
- All other laws, regulations, or policies directed at the organization and its individual users.

3. Risk Assessment

Risk assessment is a systematic process used in determining potential for and impact of a negative event by evaluating the nature of the information and information systems.

All information systems must meet the **Minimum Security Standards for Protected Information** based on the **Data Classification policy** *(see Resources below)*. Some selected systems will be designated for conducting a risk assessment at a prescribed frequency in the Schedule of Risk Assessments for Information Security (see Resources below). These selected systems will have the documented findings and any future actions placed on file for audit and accountability purposes.

4. Data Protection Requirements

Data is a valuable asset of the university, and some data must be protected with a higher level of attention and caution. The level of protection is based on the method defined by the **Data Classification policy** along with the **Minimum Security Standards for Protected Data** *(see Resources below)*.

5. Reporting of Security Incidents

A critical component of security is to address security breaches promptly and with the appropriate level of action. All individuals are responsible for reporting incidents in which they suspect data, computer or network security may have been compromised. The IT Security Incident Reporting policy (see Resources below) outlines the responsibilities of colleges, departments, units, and individuals in reporting as well as defining procedures for handling security incidents.

Resources

Links

- Acceptable Use of Information Technology Resources policy
- Electronic Privacy policy
- Information Technology Policies and Procedures
- Personal Use and Misuse of University Property policy
- Schedule of Risk Assessments for Information Security
- IT Security Incident Reporting form
- IT Security Incident Reporting policy
- Stay Cyber Safe
- Data Classification Policy
- Data Classification Standards and Guidance
- Minimum Security Standards and Guidance
- IT Glossary of Terms (DRAFT)
- IT Security [Policy in PDF with line numbers]