# ****Minimum Security Standards and Guidance****

# ****for Protection of Electronic Data****

Effective: August 1, 2015

Contact: [Information Technology Services](https://www.it.iastate.edu/)

# Contents

[Purpose](#_Toc378259792)

[1. Scope](#_Toc378259793)

[2. Audience](#_Toc378259794)

[3. Minimum Standards](#_Toc378259795)

[3.1. Minimum Standards for Account Controls](#_Toc378259796)

[3.2. Minimum Standards for System Controls](#_Toc378259797)

[3.3. Minimum Standards for Network Controls](#_Toc378259798)

[3.4. Minimum Standards for Physical Controls](#_Toc378259799)

[3.5. Minimum Standards for Training and Compliance](#_Toc378259800)

[3.6. Minimum Standards for Change Management](#_Toc378259801)

[3.7. Minimum Standards for Business Continuity](#_Toc378259802)

[4. Exceptions](#_Toc378259803)

[5. Compliance](#_Toc378259804)

[6. Resources](#_Toc378259805)

# Purpose

This standard, in concert with the [Data Classification policy](http://www.policy.iastate.edu/policy/dataclassification), implements the Data Protection Requirements section of the [Information Technology Security policy](http://www.policy.iastate.edu/policy/it/security). Adherence to these standards is an essential safeguard for the protection of electronic university data and systems. However, compliance does not assure complete security. These standards should be incorporated into a comprehensive security plan. Additional policies and laws may also apply.

# 1. Scope

This standard applies to all electronic accounts, systems, devices, and networks, which access, contain or transmit any University-owned data, to the extent that such accounts, systems, devices and networks have been made accessible to employees, agents or contractors of Iowa State Universtiy.

# 2. Audience

This standard applies to all data users, data owners, data custodians, data stewards, and system and network administrators of such accounts, systems, devices, and networks.

# 3. Minimum Standards

This section lists the minimum standards that are to be enabled and enforced for the various data protection levels.

Using the [Data Classification Standards and Guidance](http://www.policy.iastate.edu/policy/dataclassification#resources), classify each data item as restricted, high, moderate, or low.

If a reliable and effective solution is not available for a particular requirement, then a limited exception may be granted (see section 4).

## 3.1. Minimum Standards for Account Controls

These are standards related to user credentials for authentication and authorization (e.g. Net-ID, university ID).

|  |  |  |
| --- | --- | --- |
|  | **Standard** | **Data Protection Level**  |
| Restricted | **High** | **Moderate** | **Low** |
| 3.1.1 | All administrative accounts must use multifactor authentication if the technology is available and implemented. | Required | Recommended | Recommended | Optional |
| 3.1.2 | Each account must use a password meeting the ISU high level of strength. | Required | Required | Recommended | Optional |
| 3.1.3 | Each account must use a password meeting the ISU moderate level of strength. | N/A | N/A | Required | Required |
| 3.1.4 | All unused accounts must be deleted or disabled as soon as practicable. | Required | Required | Required | Recommended |
| 3.1.5 | Each account must be granted the least privilege to perform required job function(s). | Required | Required | Required | Required |
| 3.1.6 | Each account must be assigned to one individual or to one service.  | Required | Required | Required | Required |
| 3.1.7 | Each account must be restricted to a single security domain [ie. data protection level]. | Required | Recommended | Recommended | Optional |

## 3.2. Minimum Standards for System Controls

These standards are minimum best practices for systems administration.

|  | **Standard** | **Data Protection Level** |
| --- | --- | --- |
| **Restricted** | **High** | **Moderate** | **Low** |
| 3.2.1 | Local login access to the system must be restricted by access control list to those accounts with a documented business need to use the data on the system. | Required | Required | Required | Recommended |
| 3.2.2 | Remote login access to the system must be restricted to those accounts with a documented business need to use the data on the system remotely. | Required | Required | Required | Recommended |
| 3.2.3 | Accounts with access to the system will be regularly reviewed, and access removed when a business need no longer exists for that access. | Required | Required | Required | Recommended |
| 3.2.4 | Only the minimum operating system components and applications required to carry out the business function shall be installed. | Required | Recommended | Recommended | Recommended |
| 3.2.5 | Security updates to the operating system and application services shall be installed expeditiously in accordance with a consistent and prudent change management process. | Required | Required | Required | Recommended |
| 3.2.6 | If automated notification of operating system and application updates is available, it shall be enabled. | Required | Required | Required | Recommended |
| 3.2.7 | Protected data shall be stored in an encrypted form. | Required | Required | Required | N/A |
| 3.2.8 | On systems running a Microsoft Windows operating system, an approved anti-virus program must be installed, running, and have on-access scanning and automatic updates enabled. | Required | Required | Required | Recommended |
| 3.2.9 | Systems must run only the services required to perform the specific business function of the machine. | Required | Recommended | Recommended | N/A |
| 3.2.10 | Systems must not run client applications that are common attack vectors (e.g., e-mail, instant messaging, web browsers). | Required | Recommended | Recommended | N/A |
| 3.2.11 | Systems must have session timeouts and screen locks enabled. | Required | Required | Required | Optional |
| 3.2.12 | Where available, systems must run an integrity checker on critical system and configuration files. | Required | Recommended | Recommended | N/A |
| 3.2.13 | All file systems containing critical system files or protected data must require authentication and support access control. | Required | Required | Required | Recommended |
| 3.2.14 | All privileged (e.g., administrator/root) access must be logged. | Required | Recommended | Recommended | Recommended |
| 3.2.15 | All logins and logouts must be logged. | Required | Recommended | Recommended | Recommended |
| 3.2.16 | Logging of all security events is required. | Required | Recommended | Recommended | Recommended |
| 3.2.17 | Security logging must include remote logging. | Required | Recommended | Recommended | Recommended |
| 3.2.18 | Security logging must be monitored 24x7. | Recommended | Recommended | Recommended | Optional |
| 3.2.19 | Storage media and systems must be clearly labeled with Restricted Data Stickers. | Required | N/A | N/A | N/A |

## 3.3. Minimum Standards for Network Controls

These standards define network access that connect systems.

|  |  |  |
| --- | --- | --- |
|  | **Standard** | **Data Protection Level** |
| **Restricted** | **High** | **Moderate** | **Low** |
| 3.3.1 | System must be on a firewall protected network shared only with systems in the same security domain. | Required | Recommended | Recommended | Optional |
| 3.3.2 | All network transit of Protected Data across the network must be encrypted. | Required | Required | Required | N/A |
| 3.3.3 | No cleartext transmission of passwords shall be permitted. | Required | Required | Required | Required |
| 3.3.4 | Network access shall be restricted to the minimum necessary to perform required functions. (example: Firewalls) | Required | Required | Required | Optional |

## 3.4. Minimum Standards for Physical Controls

Best practices for physical securing of equipment.

|  | **Standard** | **Data Protection Level** |
| --- | --- | --- |
| **Restricted** | **High** | **Moderate** | **Low** |
| 3.4.1 | Systems must be located in a locked room with limited access. | Required | Recommended | Recommended | N/A |
| 3.4.2 | Systems must be located in a locked rack or cage. | Required | Optional | Optional | Optional |
| 3.4.3 | Backup media must be physically secured from unauthorized access. | Required | Required | Required | Recommended |
| 3.4.4 | Backup media must be stored in a physically diverse location. | Required | Recommended | Recommended | Recommended |
| 3.4.5 | Systems must be provided with power protection (conditioning, uninterruptable power supply [UPS], and backup generator). | Required | Recommended | Recommended | Optional |
| 3.4.6 | Systems must be located in a room with appropriate environmental (e.g., heat and humidity) controls. | Required | Recommended | Recommended | Recommended |
| 3.4.7 | Systems storage media must be securely erased or disposed of when system function/role changes including equipment disposal. | Required | Required | Required | Recommended |
| 3.4.8 | Storage media must be physically destroyed when system function/role changes to a lower classification or at equipment disposal. | Required | Recommended | Recommended | N/A |

## 3.5. Minimum Standards for Training and Compliance

These are the steps necessary to ensure security policy and standard awareness.

|  |  |  |
| --- | --- | --- |
|  | **Standard** | **Data Protection Level** |
| **Restricted** | **High** | **Moderate** | **Low** |
| 3.5.1 | All system users must be notified of what protected data exists on a system and its protection requirements. | Required | Recommended | Recommended | N/A |
| 3.5.2 | At least annually all system users must sign the *Protected Data Confidentiality Agreement. [link pending]* | Required | Recommended | Recommended | N/A |

## 3.6. Minimum Standards for Change Management

Standards related to approved changes to systems.

|  |  |  |
| --- | --- | --- |
|  | **Standard** | **Data Protection Level** |
| **Restricted** | **High** | **Moderate** | **Low** |
| 3.6.1 | System administrators must establish, document and use an approved change control process for system configuration. | Required | Recommended | Recommended | Recommended |
| 3.6.2 | System changes and patches must be evaluated and tested prior to installation in a production environment. | Recommended | Recommended | Recommended | Recommended |

## 3.7. Minimum Standards for Business Continuity

This ensures the availability of university data and information processing systems.

|  |  |  |
| --- | --- | --- |
|  | **Standard** | **Data Protection Level** |
| **Restricted** | **High** | **Moderate** | **Low** |
| 3.7.1 | System administrators must establish, document, and follow a regular backup schedule. | Required | Recommended | Recommended | Recommended |
| 3.7.2 | The ability to restore from backup must be tested at least once a month (automated verification, user-initiated, or trial restores are acceptable methods). | Required | Recommended | Recommended | Recommended |
| 3.7.3 | Follow [IT Security Incident Reporting Policy](http://www.policy.iastate.edu/policy/it/incident) upon discovery of possible compromised data.  | Required | Required | Required | Recommended |

# 4. Exceptions

If any of the required minimum standards cannot be met, a *Security Exception Plan [link pending]*, which reports the non-compliance and describes the plan for risk assessment and mitigation, must be filed with the Information Security Office for approval. Upon approval of the plan, a limited exception may be granted.

# 5. Compliance

Non-compliance with these standards will result in revocation of access to the data, system, and/or network, as well as notification of superiors.

All Iowa State University employees are required to comply with all applicable policies, standards, rules, regulations and laws.

# 6. Resources

# [Data Classification Policy](http://www.policy.iastate.edu/policy/dataclassification)

[Data Classification Standards and Guidance [DOCX]](http://www.policy.iastate.edu/policy/dataclassification#resources)

[Data Governance Committee [DOCX]](http://www.policy.iastate.edu/sites/default/files/resources/Data%20Governance%20Committee%20Charter%202013-07-26%20aw.docx)

Information Security Office (email)

[Information Technology Security Policy](http://www.policy.iastate.edu/policy/it/security)

[IT Security Incident Reporting Policy](http://www.policy.iastate.edu/policy/it/incident)

[IT Glossary of Terms](http://www.it.iastate.edu/policies/glossary)

Implementation Guidelines (link pending)