THE UNIVERSITY OF IOWA INFORMATION SECURITY PLAN

This document is a compilation of resources, policy information and descriptions encompassing the overall (enterprise) information security environment at The University of Iowa.

Individual units are expected to develop plans which are scoped to the specific environment requiring the completion of a **System Security Plan** (SSP), as a requirement of the Federal Information Security Management Act (FISMA) of 2002.

Provided by:

Jane Drews, CISO

University of Iowa
Information Security & Policy Office
2800 UCC, Iowa City, IA 52242
it-security@uiowa.edu

Revised May 2017

Contents

IDENTIFICATION & CONTACTS

Enterprise Information Technology Contact

Steve Fleagle, Associate Vice President and University Chief Information Officer:
steve-fleagle@uiowa.edu or 319-384-0750, 2800 UCC

Assignment of Enterprise Security Responsibility

Jane Drews, University Chief Information Security Officer:
jane-drews@uiowa.edu or 319-335-5537, 2800 UCC

NOTE: Individual applications and systems will also have one or more local information technology contacts responsible for the management/administrative, operational, and technical controls implementation, and will also assign a person(s) for operational IT security responsibility.

SENSITIVITY OF INFORMATION

Determining Information Sensitivity

Use the following table to determine if a collection of information is classified as Level I (Low Sensitivity), Level II (Moderate Sensitivity), or Level III (High Sensitivity). Additional guidance for classifying a particular information system can be found at the Institutional Data Classification Guidelines: https://itsecurity.uiowa.edu/classifying-institutional-data

University of Iowa Policy:
Institutional Data Access: https://itsecurity.uiowa.edu/policy-institutionaldataaccess

University of Iowa Data Classifications			
Need for:	***LEVEL I*** ***Low Sensitivity*** ***(Limited Adverse Effect)***	***LEVEL II*** ***Moderate Sensitivity*** ***(Serious Adverse Effect)***	***LEVEL III*** ***High Sensitivity*** ***(Severe/Catastrophic Adverse Effect)***
Confidentiality Preserving authorized restrictions on data access and disclosure	**Low** Optional Public Data	**Medium** Recommended Non-Public or Internal Data	**High** Required Confidential/Restricted Data
	AND/OR	**AND/OR**	**AND/OR**
Integrity Preventing improper modification or destruction and preserving authenticity of data	**Low Risk** Optional Easily Reproducible	**Medium Risk** Recommended Internally Trusted	**High Risk** Required Official or Highly Trusted Data
	AND/OR	**AND/OR**	**AND/OR**
Availability Ensuring timely and reliable access to and use of data	**Low Impact** Optional Informational or Non-Critical	**Medium Impact** Recommended Normal Services	**High Impact** Required Critical or Campus-wide service

MANAGEMENT/ADMINISTRATIVE CONTROLS

Risk Assessment (RA)

Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of information systems and the associated processing, storage, or transmission of information.

University of Iowa Information Security Program: https://itsecurity.uiowa.edu/resources/faculty-staff/enterprise-information-security-program Section 2.1, also see page 10 of this document.

University of Iowa Policy:
Computer Vulnerability Scanning: https://itsecurity.uiowa.edu/scan-pen-test

Planning (PL)

Organizations must develop, document, periodically update, and implement security plans for information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

University of Iowa Information Security Program: https://itsecurity.uiowa.edu/resources/faculty-staff/enterprise-information-security-program Section 2.4, also see page 10 of this document.

University of Iowa Policy:
Information Security Framework: https://itsecurity.uiowa.edu/policy-information-security-framework
Acceptable Use of Information Technology Resources: https://opsmanual.uiowa.edu/community-policies/acceptable-use-information-technology-resources

System and Services Acquisition (SA)

Organizations must: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

University of Iowa Policy:
Information Security Framework: https://itsecurity.uiowa.edu/policy-information-security-framework (Information Integrity Controls Section)
Acceptable Use of Information Technology Resources: https://opsmanual.uiowa.edu/community-policies/acceptable-use-information-technology-resources (Section 19.4)

Security Assessment and Authorization (CA)

Security assessments: (i) ensure that information security is built into organizational information systems; (ii) identify weaknesses and deficiencies early in the development process; (iii) provide essential information needed to make risk-based decisions as part of security authorization processes; and (iv) ensure compliance to vulnerability mitigation procedures.

University of Iowa Policy:
Information Security Framework: https://itsecurity.uiowa.edu/policy-information-security-framework (Information Assessment and Classification Section)
Network Vulnerability Scanning and Penetration Testing https://itsecurity.uiowa.edu/scan-pen-test
Enterprise Information Security Program https://itsecurity.uiowa.edu/resources/faculty-staff/enterprise-information-security-program

OPERATIONAL CONTROLS

Personnel Security (PS)

Organizations must: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

University of Iowa Policy:
Criminal Background Checks: https://opsmanual.uiowa.edu/human-resources/hiring-and-appointments/criminal-background-check-point-hire (Section 9.3)
https://opsmanual.uiowa.edu/human-resources/hiring-and-appointments/credential-check-point-hire (section 9.2)
Confidentiality Agreements: https://itsecurity.uiowa.edu/policy-information-security-framework (Information Access Section)
https://itsecurity.uiowa.edu/sites/itsecurity.uiowa.edu/files/wysiwyg_uploads/policy-confidentiality-stmt.pdf
Employee Termination Procedures:
https://hr.uiowa.edu/policies/termination-procedures, https://hr.uiowa.edu/hr-unit-reps/employee-exit-process
Acceptable Use of Information Technology Resources: https://opsmanual.uiowa.edu/community-policies/acceptable-use-information-technology-resources (Section 19.5)

Physical and Environmental Protection (PE)

Organizations must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

University of Iowa Policy:
Information Security Framework: https://itsecurity.uiowa.edu/policy-information-security-framework (Information Access Section)
Institutional Data Access: https://itsecurity.uiowa.edu/policy-institutionaldataaccess

Contingency Planning (CP)

Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

University of Iowa Enterprise Level Information Technology Disaster Plan:
https://itsecurity.uiowa.edu/sites/itsecurity.uiowa.edu/files/enterprise-it-disaster-plan.pdf
https://itsecurity.uiowa.edu/resources/system-administrators-and-it-managers/drbcp

University of Iowa Policy:
Information Security Framework: https://itsecurity.uiowa.edu/policy-information-security-framework (Preventive Measures, Backup, and Recovery Section)
Backup and Recovery: https://itsecurity.uiowa.edu/policy-backup-recovery

Configuration Management (CM)

Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.

University of Iowa Policy:
Information Security Framework: https://itsecurity.uiowa.edu/policy-information-security-framework (Information Integrity Section)

Maintenance (MA)

Organizations must: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

University of Iowa Policy:
Information Security Framework: https://itsecurity.uiowa.edu/policy-information-security-framework (Information Access Section)

System and Information Integrity (SI)

Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

Anti-Spam/Anti-Virus Services: https://its.uiowa.edu/antivirus

University of Iowa Policy:
Information Security Framework: https://itsecurity.uiowa.edu/policy-information-security-framework (Information Integrity Controls Section)

Media Protection (MP)

Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.

University of Iowa Policy:
Information Security Framework: https://itsecurity.uiowa.edu/policy-information-security-framework (Data Disposal Section)
Computer Data and Media Disposal: https://itsecurity.uiowa.edu/computerequipmentdisposal
Institutional Data Access: https://itsecurity.uiowa.edu/policy-institutionaldataaccess

Incident Response (IR)

Organizations must: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.

University of Iowa Computer Incident Response Team:
https://itsecurity.uiowa.edu/i-csirt
https://itsecurity.uiowa.edu/sites/itsecurity.uiowa.edu/files/i-csirt-flowchart.pdf

University of Iowa Policy:
IT Security Incident Escalation: https://itsecurity.uiowa.edu/it-security-incident-escalation
Computer Security Breach Notification: https://itsecurity.uiowa.edu/computer-security-breach-notification-policy
Roles and Responsibilities: https://itsecurity.uiowa.edu/policy-roles-and-responsibilities

Awareness and Training (AT)

Organizations must: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

University of Iowa Policy:
Roles and Responsibilities: https://itsecurity.uiowa.edu/policy-roles-and-responsibilities

A Security Awareness Training Course is available and recommended to all members of the University of Iowa community: https://itsecurity.uiowa.edu/resources/everyone/learnaboutsecurity

TECHNICAL CONTROLS

Identification and Authentication (IA)

Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

University of Iowa Policy:
Information Security Framework: https://itsecurity.uiowa.edu/policy-information-security-framework (Information Access Section)
Login ID Standard: https://itsecurity.uiowa.edu/enterprise-login-id-standard
Passwords: https://itsecurity.uiowa.edu/enterprise-password
Roles and Responsibilities: https://itsecurity.uiowa.edu/policy-roles-and-responsibilities

Access Control (AC)

Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

University of Iowa Policy:
Information Security Framework: https://itsecurity.uiowa.edu/policy-information-security-framework (Information Access Section)
Roles and Responsibilities: https://itsecurity.uiowa.edu/policy-roles-and-responsibilities

Audit and Accountability (AU)

Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

University of Iowa Policy:
Information Security Framework: http://itsecurity.uiowa.edu/policy/policy-information-security-framework.shtml (Audits Section, Preventive Measures, Backup, and Recovery Section)
Institutional Data Access: http://itsecurity.uiowa.edu/policy/policy-InstitutionalDataAccess.shtml
Backup and Recovery: http://itsecurity.uiowa.edu/policy/policy-backup-recovery.shtml

System and Communications Protection (SC)

Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

University of Iowa Policy:
Information Security Framework: https://itsecurity.uiowa.edu/policy-information-security-framework (Communications Security Section)

Enterprise Information Security Program

PART 1: OVERVIEW AND SECURITY PROGRAM OBJECTIVES

The University of Iowa's program for information security is a combination of policy, security architecture modelling, and descriptions of current IT security services and control practices. When integrated, the overall program describes **administrative**, **operational**, and **technical** security safeguards that must be implemented for/in information systems involved in the processing and storage of sensitive or private information.

The Security Program provides business value by enabling the delivery of applications to more individuals, in a timelier manner, with integral data. Appropriate information security is crucial to this environment, in order to manage the risks inherent in a distributed, open computing environment.

The practice of "**Defense in Depth**" is utilized at the University of Iowa, providing several different layers of protection, each working to contribute to the overall protection of information assets:

1. Information integrity and access controls
2. Application logic, error checking, and data validation controls
3. Server and client based logical and physical protections
4. Internal and perimeter network level protections
5. Employee policy, practices, and procedures

Business Owners, along with the University Information Security and Policy Office, are responsible for taking appropriate steps to assess internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of institutional data. Risks in a large and diversified computing environment may include, but are not limited to:

- Unauthorized access to sensitive or confidential institutional information
- Compromised computer system(s) integrity as a result of access by an intruder
- Interception of data traversing network(s)
- Physical loss of data center, infrastructure, facilities, or computer equipment
- Errors or other corruption introduced into computer systems or applications
- Inadequate system administration support practices
- Loss of system availability

Responsibility for managing the University Information Security Program is described in the **Roles and Responsibilities for Information Security Policy(2).** This program description will be reviewed and updated as necessary on an annual basis by the University Chief Information Security Officer. The revisions and reviews of this program will be recorded in the table included as **Appendix A**. In addition, documentation supporting the University's compliance with regulatory controls, as appropriate, will be maintained by the Information Security and Policy Office. This may include audit reports, assessment reports, and other documents that are prepared.

PART 2: SECURITY PROGRAM CONTROL AREAS

Risk Assessment and Planning

Risk assessments are performed on critical information technology assets of the University of Iowa on a regular basis by both the University of Iowa Internal Audit department, and by the Office of the State Auditor. Feedback includes a comprehensive report of actionable risk mitigation/remediation

recommendations.

The Information Security and Policy Office also performs technical risk assessments, and/or penetration tests for management and business owners upon request, which are conducted and maintained in a strictly confidential manner. In addition, a formalized process for approving IT security plans for research, prior to (contract) agreements, grants, and other relationships or collaborations with the University of Iowa is available, which includes a security risk assessment phase.

The Information Security and Policy Office will, in addition, facilitate an entity wide security risk assessment, as necessary whenever significant changes to the computing environment are implemented, or minimally within five years.

Security must be a consideration from the very beginning of any project at the University rather than something that is added later. The Information Security and Policy Office is a resource available to assist with this effort throughout the planning phase of a project. In addition, a control review should be performed before implementation of computer systems which house or handle confidential institutional information. This may include a:

- technical security evaluation to ensure appropriate safeguards are in place and operational
- risk assessment, including a review for regulatory, legal, and policy compliance
- contingency plan, including the data recovery strategy
- review of on-going production procedures, including change controls and integrity checks
- penetration test to evaluate and ensure controls operate as expected

The University **Network Vulnerability Scanning and Penetration Testing Policy** describes the types of network based assessments conducted by the Information Security and Policy Office to determine the effectiveness of controls and management of systems connected to the University data network.

Security Policy

All IT policy, under the review and approval of the University Chief Information Officer, is included in the University Operations Manual via the **Acceptable Use of Information Technology Resources Policy (5)** which describes the expectations for all members of the user community for appropriate use of technology, protection of privacy, and protection of academic freedoms. The University of Iowa has developed a process for development, review, and approval of IT policy, which is documented at https://itsecurity.uiowa.edu/university-it-policy/about-university-it-policy.

The University provides an annual campus e-mail notification to all members of the University community describing a selection of important IT policies. The notification also directs them to the IT policy repository as an additional educational measure, and includes key aspects of policy in the computer based security awareness program offered to campus personnel.

Organization of Information Security

The **Role and Responsibilities for Information Security Policy (2)** describe the overall organization at the University of Iowa. In addition, the information security architecture model below describes the local and enterprise level services, technologies, responsibilities and techniques in use.

All Information Technology Services personnel are required to sign a data confidentiality agreement at hire time, and annually thereafter via the Employee Self-Service web application. The statement is available at https://itsecurity.uiowa.edu/sites/itsecurity.uiowa.edu/files/wysiwyg_uploads/policy-confidentiality-stmt.pdf

Information Security Architecture Model

LOCAL	End-Users	Promptly report problems Keep all software up to date Use complex passwords	Observe acceptable use policy Use a workstation (personal) firewall Complete security awareness training	Practice safe email & web browsing Store confidential data on servers Use computer Lockout/screen savers
	Applications	Plan for appropriate security Develop and test disaster plans Implement data handling controls	Implement scoped access controls Use SDLC/change management Enable logging of security event/activity	Observe strict media protection controls Produce and Test backups
	Security Auditing, Monitor, Investigate	Intrusion Detection/Prevention Incident response procedures, Forensics, CSIRT team	Risk assessments SEM/Logging & Correlation	Network and Application Scanning Metrics
ENTERPRISE	Security Technologies	Active Directory, LDAP, Kerberos, Shibboleth Firewalls Anti-virus, Anti-Malware	VPN ILM & IdM/Provisioning SSL Certificates	IDS/IPS SCCM, SCOM NAC/Segmentation
	Security Services	Identification Authorization Confidentiality	Authentication Access Controls Data Classification	Data Integrity & Data Handling Encryption & Non-Repudiation Awareness & Training
	Security Policy & Standards	Acceptable Use Institutional Data Network Citizenship Passwords	Security Framework Roles & Responsibilities Security Incident Escalation & Notification Login IDs	Backups Data & Media Disposal Background Checks Wireless

Asset Management

The **Information Security Framework Policy (1) Institutional Data Access Policy (3)**, data handling procedures, and the **Roles and Responsibilities Policy (2)** describe individual responsibilities for managing and inventorying our physical and logical assets.

A tool is available to assist business owners of institutional data to appropriately classify the sensitivity of their information. These guidelines are available at https://itsecurity.uiowa.edu/resources/everyone/determining-risk-levels. Once a set of institutional data is classified, appropriate protections can be applied.

In addition, University Administration have developed a policy regarding the use and protection of **Social Security numbers (14)**, regarded as highly sensitive data.

Personnel Security

The University of Iowa has implemented a policy and program to perform **Credential and Criminal Background checks (4)** when filling all security sensitive positions, at point of hire. The policy includes the necessary consent documents and procedures.
A computer based, self-enrolled, Computer Security Awareness Program is available to all University employees, through the Employee Self-Service Portal (https://hris.uiowa.edu) "**My Training**" resources.

A marketing campaign is conducted regularly to raise awareness of its availability, along with other directed reminders. In addition, security seminars are offered to campus IT staffs, as well as a "**Security Day**" training event. Poster and postcard campaigns are also used; with prominent links to the main IT Security website https://itsecurity.uiowa.edu.

Specialized training is also offered, for privacy issues related to standards and regulations such as Family Education rights and Privacy Act **(FERPA)**, Health Insurance Portability and Accountability Act **(HIPAA)**, and Payment Card Industry Data Security Standards **(PCI-DSS)**.

The University Human Resources department maintains information related to the employee exit process (terminations and transfers), which includes policy and forms, at the following location: https://hr.uiowa.edu/hr-unit-reps/employee-exit-process

Automated provisioning and de-provisioning guidelines for University community members are available at http://its.uiowa.edu/statuschanges.

Physical Security Measures

The University **Information Security Framework Policy (1)** has a section under Information Access that describes physical security requirements. In addition, requirements for preventive measures, emergency operations, and mobile devices are outlined.

The **Computer Data and Media Disposal Policy (7)** describes the requirements for physical security of equipment and data when it leaves owner control. Best practices for the secure removal of data are at https://itsecurity.uiowa.edu/computerequipmentdisposal, and the Security Office offers a training program for IT staffs involved with transfers or disposals of equipment.

The **Backup and Recovery Policy (6)** describes requirements for backups, including off-site storage of media.

Communication and Operations Management

The **Information Security Framework Policy (1)** includes a section on information integrity controls which includes requirements for segregation of critical functions, maintenance of systems and applications software, change management procedures for applications, as well as anti-malware control requirements. In addition, automated operations and contractor access are outlined, as well as auditing

and logging requirements and communications security requirements.

The **Institutional Data Access Policy (3)** describes data handling controls for various sensitivity levels of data, the **Backup and Recovery Policy (6)** outlines requirements for backups, and the **Computer Data and Media Disposal Policy (7)** describes requirements for secure disposal of information. The University Records Management Program at https://fmb.fo.uiowa.edu/records-management has information regarding the retention of university records.

Access Control

The **Information Security Framework policy (1)** outlines requirements for information access in the electronic access control section. In addition, the standard format for Login Identifiers (user names) is described in the **Enterprise Login ID standard (10)**, and the policy requirements for authentication are in the **Password Policy (9)**. The UI Policy describing the classification scheme for institutional data, and the data handling controls required for each level of data, is outlined in the **Institutional Data Access policy (3)**. Requirements for systems attached to the University data network are described in the **Network Citizenship Policy (11)**.

The University provides a Virtual Private Network (VPN) service for secure off-site access to university resources, which is described at https://its.uiowa.edu/vpn

Systems Development and Maintenance

Information Integrity Controls are described in the **Information Security Framework Policy (1)** and include separation of duties and functions, emergency access procedures, system and application management process, and software development change management procedures. Information regarding encryption is also described, with additional resources and assistance at the Encryption Support Center: https://its.uiowa.edu/encryption

Disaster Recovery and Business Continuity Management

An enterprise level disaster recovery plan overview has been developed and is available at https://itsecurity.uiowa.edu/sites/itsecurity.uiowa.edu/files/enterprise-it-disaster-plan.pdf. This resource includes a methodology for developing unit-level disaster plans to compliment the university plan. A sample set of planning forms template is available for units at https://itsecurity.uiowa.edu/resources/system-administrators-and-it-managers/drbcp.

Preparing for emergency operations and business continuity is also described in the Information **Security Framework Policy (1)**. The University of Iowa also maintains a Critical Incident Management Plan at https://opsmanual.uiowa.edu/administrative-financial-and-facilities-policies/critical-incident-management-plan.

Information Security Incident Response

The University of Iowa has an incident response capability which is documented at the IT Security website https://itsecurity.uiowa.edu/incidents along with a policy describing **Security**

Incident Escalation Procedures (12) for security incident resolution. The University's policy regarding **Computer Security Breach Notification (13)** is available. The Information Security and Policy Office has analysts available via our on-call process to assist with security incident response, forensic analysis, e-discovery requests, and to aid in controlling liability to the university in the event of a breach.

A university-wide **Iowa Computer Security Incident Response Team (I-CIRT)** program is described at https://itsecurity.uiowa.edu/i-csirt and is utilized in the event of a significant IT incident requiring campus wide coordination and response.

The Information Security and Policy Office provides continuous monitoring of the university data network for malicious activity, and reports problems as they arise to department network/security contacts (NSC's) within each unit, who are liaisons to the Information Security and Policy Office for security and networking issues.

The NSC program is described at https://itsecurity.uiowa.edu/incidents/know-your-responsibilities-nsc. In addition, the Information Security and Policy Office allows system owners to individually provide contact information in the event of problems, described at https://itsecurity.uiowa.edu/services/usr. A scanning service is also maintained to assist with determination of vulnerabilities in systems and applications.

Compliance

The following regulations pertain to information security and privacy, to which all or part of the University's electronic information applies:

- Family Education Rights and Privacy Act **(FERPA)** https://registrar.uiowa.edu/ferpa
- Health Insurance Portability & Accountability Act **(HIPAA)**
- https://itsecurity.uiowa.edu/university-it-policy/hipaa
- Gramm Leach Bliley Act **(GLBA)** http://counsel.cua.edu//fedlaw/glb.cfm
- Payment Card Industry Data Security Standards **(PCI-DSS)** https://www.pcisecuritystandards.org/pci_security/
- UI Policy on Credit Cards https://treasury.fo.uiowa.edu/policies-and-procedures
- Federal Information Security Management Act **(FISMA)** http://csrc.nist.gov/groups/SMA/fisma/overview.html
- Iowa Personal Information Security Breach Notification (Iowa Code, Title XVI, Chapter 715C)

The Information Security and Policy Office assists all University units and areas with assessments and testing methods to ensure compliance with all applicable privacy and security regulations.

PART 3: INFORMATION TECHNOLOGY POLICY - https://itsecurity.uiowa.edu/university-it-policy

1. Information Security Framework
   https://itsecurity.uiowa.edu/policy-information-security-framework
2. Roles and Responsibilities for Information Security
   https://itsecurity.uiowa.edu/policy-roles-and-responsibilities
   Institutional Data Access Policy

https://itsecurity.uiowa.edu/policy-institutionaldataaccess

3. Criminal Background and Credential Checks Policy https://opsmanual.uiowa.edu/human-resources/hiring-and-appointments/criminal-background-check-point-hire
   Acceptable Use of Information Technology Resources Policy https://opsmanual.uiowa.edu/community-policies/acceptable-use-information-technology-resources
4. Backup and Recovery Policy https://itsecurity.uiowa.edu/policy-backup-recovery
5. Computer Data and Media Disposal Policy https://itsecurity.uiowa.edu/computerequipmentdisposal
6. Credit Card Policy http://treasury.fo.uiowa.edu/policies-and-procedures
7. Password Policy https://itsecurity.uiowa.edu/enterprise-password
8. Login ID policy https://itsecurity.uiowa.edu/enterprise-login-id-standard
9. Network Citizenship Policy https://itsecurity.uiowa.edu/networkcitizenship
10. Security Incident Escalation Policy https://itsecurity.uiowa.edu/it-security-incident-escalation
11. Security Breach Notification Policy https://itsecurity.uiowa.edu/computer-security-breach-notification-policy
12. SSN policy https://opsmanual.uiowa.edu/community-policies/social-security-numbers
13. Network Vulnerability Scanning and Penetration Testing policy https://itsecurity.uiowa.edu/scan-pen-test

The University of Iowa Defense in Depth Security Strategy

Defense in depth, at The University of Iowa, is a combination of controls implemented at the Enterprise level, at the Service Provider level, and at the End User level.

The "Defense in Depth" operational philosophy and architectural design for securing information technology systems, services, and processes is a *multi-layered* strategy that encompasses administrative and personnel controls, technology controls, and operational controls covering a broad spectrum including, but not limited to, perimeter defences, network security, host/platform security, and application security.

Defense in Depth involves a tiered approach in defense mechanisms. Each protection layer has unique characteristics, presenting obstacles for an intruder to overcome, (as well as preventing accidents by a legitimate user), if s/he attempts to circumvent controls over confidentiality, availability, and integrity of information assets. If one protection layer fails, the next (or the next) should prevent a breach in security. Defense in depth provides "compound" protection, rather than the simple "sum" of all protections.

Enterprise's Responsibility

1. A security incident response capability has been developed to assist with detection and response to information technology related problems.
2. Intrusion detection systems are deployed to monitor the network for anomalous activities.
3. Antiviral and anti-spam protections are deployed at the gateway to the campus.
4. Network filtering is employed to block "known bad" or high-risk traffic (i.e., spoofed/forged addresses, RDP and SSH protocols, and the well-known Microsoft networking ports).
5. Identity management and provisioning of services is offered, for timely granting/revocation of access to confidential data.
6. Network based vulnerability assessments (i.e., scanning) are performed on a regular basis and communicated to applicable IT staff members.
7. Technology security training and awareness seminars, classes, and materials are developed and offered to the University community.
8. Risk assessments that target critical systems and services offered by the University are regularly performed.
9. Employee background checks are performed, and confidentiality agreements are signed by all staff involved with support of enterprise services.
10. System hardening is employed to ensure that only the necessary services are enabled on systems that support enterprise services, the least-privilege principle is used for granting access, and strict patch/update management principles are followed, using documented change management procedures.
11. Separation of critical duties is required, and no "single person dependencies," are allowed (i.e., a minimum of two persons have privileged access to systems, and at least two persons must be involved in critical service maintenance operations).
12. A documented disaster recovery and business resumption plan exists and is regularly tested.
13. Licenses for security software (ssh, ssl, iss, sftp, etc) are purchased or subsidized to promote broad campus use of encrypted protocols and security services.

Service Provider's Responsibility

1. All institutional data is reviewed and classified by the data owner as to its confidentiality using University guidelines; security and access controls are based on the data classification and least privilege principle.
2. System hardening is employed to ensure that only the necessary services are enabled on systems, the least-privilege principle is used for granting access, strict patch/update management principles are followed, using documented change management procedures, and firewalls, IP restrictions or filters are employed where possible to limit system access to known users.
3. Software development (programming) is performed on non-production systems using documented change management procedures for production deployment.
4. Secure (encrypted) protocol alternatives are deployed in place of insecure protocols (i.e., ssh instead of telnet, sftp in place of ftp).
5. Auditing of system activity is performed, accompanied by regular reviews of exception activity and login activity on each system.
6. Adequate backup and recovery systems are in place, in accordance with University policy.
7. Separation of critical duties is required, and no "single person dependencies," are allowed (i.e., a minimum of two persons have privileged access to systems, and at least two persons must be involved in critical service operations).
8. Employee background checks are performed, and confidentiality agreements are signed by IT support staff.
9. All institutional technology security policies are communicated, understood, and adhered to by IT staff.
10. A contingency plan and data recovery procedures are documented and regularly tested.
11. Enterprise identity management services are employed for authentication, using "HawkID" identifiers, where technically feasible.

End User's Responsibility

1. Good password management is used at all times: passwords are changed often, never reused, and difficult to guess, and contain a long combination of letters, numbers, and other characters.
2. Automatic updating for software service patches is enabled, if possible; and updates are always installed immediately when prompted or when directed (by management) to do so.
3. Anti-virus software is installed, and auto-updated on a daily basis.
4. Workstations are either logged off or shut down when not in use overnight and on weekends.
5. Automatic inactivity locking is enabled by activating a password-protected screen saver after 10 minutes during the work day.
6. Suspicious, unusual, or unexplainable activity in the workplace, on your computer, or elsewhere in your area is always promptly reported to your supervisor or if your supervisor is not available, to the Information Security and Policy Office (for computer activity) or to Public Safety (for workplace activity).
7. Confidential data is only shared with authorized personnel, and never used for purposes other than originally intended.
8. Backup copies of important files and documents are created according to departmental procedures.
9. Only hardware and software that has been purchased for your use, by your department on your workstation, is installed and used.
10. All default operating system services and programs that are not needed in the course of your job are disabled on your workstation (e.g., personal web server, ftp server, message service).
11. Software programs downloaded from a web site, or received as an attachment via email are never opened or used/installed unless it has been virus-scanned first.
12. The University's Acceptable Use of Information Technology Resources policy is read and understood.

13. All confidential or sensitive data is removed from your workstation before it leaves your control (e.g., going to surplus or as a department hand-me-down), including software for which only you have a license.

Supporting IT Security Program, Policy, Best Practice, and Procedure Documents:

Information Security & Policy Office Website: https://itsecurity.uiowa.edu/

Information Technology Policy Website: https://itsecurity.uiowa.edu/university-it-policy