Information Security Policy Manual

Latest Revision: May 16, 2012

Table of Contents

Information Security Policy Manual

The University of Connecticut developed information security policies to protect the availability, integrity, and confidentiality of University information technology (IT) resources. While these policies apply to all faculty, staff, and students of the University, they are primarily applicable to Data Stewards, those that manage access to data and IT resources, and those who use University IT resources.

The University expects all employees, students and users to adhere to the policies herein. No set of policies can address all scenarios of IT security; therefore, these policies address the most common aspects of security. We cannot eliminate malevolent behavior or irresponsibility, but we can guide users and administrators toward responsible decisions and actions.

The Chief Information Security Officer (CISO) manages the University's information security activities. The CISO works in cooperation with University employees whose responsibilities address information technology and information security.

In order to protect resources from threats and ensure compliance with applicable laws and industry standards, the University will manage and regulate networks and other IT resources.

All employees must immediately report lost or stolen technology resources to the University Police Department (860-486-4800), the Information Security Office (860-486-8255), and the Office of the Controller (860-486-2937).

The University's IT resources, whether owned or contracted, will be configured to meet the requirements set forth in these policies. Agreements that involve a third party accessing or managing the University's IT resources shall comply with all of the requirements specified in these policies.

Owners of IT resources are responsible for keeping computer systems protected from activities that could compromise the confidentiality, integrity, or availability of the resources. Owners shall perform regular and timely computer maintenance, which includes, but is not limited to, installation of software patches, and updates to malware and virus protection. The automatic implementation of patches and updates at regular intervals will be utilized for all capable devices. Owners of IT resources should be aware of the business and availability requirements for their systems, and owners shall create appropriate documentation and processes to meet the requirements outlined in these policies.

University managers should direct faculty and staff to the information security policies and discuss the impacts and outcomes of the policies for their specific areas. Upon hire, employees will sign a "Statement of Policy Acknowledgement" which will be administered and maintained by the Human Resources department.

The regulations of *The Student Code* remain applicable to students and their registered organizations, regarding information security:

> *"Unauthorized possession, duplication, or misuse of University property or other personal or public property, including but not limited to records, electronic files, telecommunications systems, forms of identification, and keys."* (Student Code, III. Proscribed Conduct, Section B, 16)

Contact

Chief Information Security Officer, Jason Pufahl: Jason.pufahl@uconn.edu / (860) 486-3743

Please email security@uconn.edu for questions, concerns or general feedback.

Please email abuse@uconn.edu to report any security breaches or incidents.

Please visit http://security.uconn.edu for more information.

Enforcement

Violations of information security policy may result in appropriate disciplinary measures in accordance with local, state, and federal laws, as well as University Laws and By-Laws, General Rules of Conduct for All University Employees, applicable collective bargaining agreements, and the University of Connecticut Student Conduct Code.

For purposes of protecting the University's network and information technology resources, the Information Security Office may temporarily remove or block any system, device, or person from the University network that is reasonably suspected of violating University information security policy. These non-punitive measures will be taken only to maintain business continuity and information security, and users of the University's information technology resources will be contacted for resolution.

Any individual who suspects a violation of this policy may report it to:

- The Information Security Office: (860) 486-8255
- The Compliance Office in the Office of Audit, Compliance and Ethics: (860) 486-4526
- Anonymously through the Reportline: (888) 685-2637 or https://www.compliance-helpline.com/uconncares.jsp.

Policies And Related Procedures

1. ACCEPTABLE USE

The Acceptable Use policy is intended to supplement the State of Connecticut Acceptable Use policy and applies to all users of the University's computer and network resources.

Information technology (IT) resources must be utilized respectfully and as authorized and designed. While utilizing University-owned IT resources, no user or administrator is authorized to engage in any activity that violates University policy or any illegal activity under local, state, federal or international law.

Users and administrators may not engage in any activity that interrupts personal productivity or the service of any University resources. Users and administrators will not intentionally disrupt, damage, or alter data, software, or other IT resources belonging to the University or to any other entity. This includes spreading viruses, sending spam messages, performing denial of service attacks, compromising another individual's ability to use IT resources, and performing system/network reconnaissance.

Users of University systems shall not tamper with, disable, or circumvent any security mechanism, including software applications, login account controls, network security rules, hardware devices, etc.

Users shall not introduce any prohibited information technology resources that could disrupt operations or compromise security of the University's IT resources.

2. ACCESS CONTROL POLICY

All University information technology (IT) resources that store, process, or transmit Confidential or Protected data must require usernames and passwords for access.

Data Stewards must authorize all individuals prior to their accessing IT resources that store, process or transmit Confidential or Protected Data.

Individual units are responsible for developing and implementing procedures for authorizing and granting access to their IT resources that store, process or transmit Confidential or Protected Data.

Data Stewards shall document all data access privileges, and will reevaluate access privileges when a user's job assignment changes. When a user no longer requires data access or leaves the University for any reason, the Data Steward shall revoke the user's access privileges. The user's supervisor is responsible for making appropriate and timely requests to the Data Steward for IT resource account access modification.

Individuals with access to Confidential or Protected Data may not share or redistribute this data without receiving the expressed, prior consent of the Data Steward.

Login Names and Passwords

Data Administrators will configure systems and applications to meet the following requirements to authentic users of IT resources that store, process or transmit Confidential or Protected Data:

- Data Administrators must assign each user a unique login name.
- Login names will have an associated password, which is required to minimally meet the standards outlined in the University password standards.

Users must not share account passwords with any other person.

Review & Compliance

For systems where Confidential Data is stored, processed, or transmitted, Data Stewards and Data Administrators will review user access rights annually using a documented process.

Data Stewards, or their designated representatives, shall ensure appropriate procedures are documented, disseminated, and implemented to ensure compliance with this policy.

3. DATA ROLES AND RESPONSIBILITIES

Data Stewards oversee the proper handling of administrative, academic, public engagement, or research data. Data Stewards are responsible for classifying data according to the University's data classification system, ensuring that appropriate steps are taken to protect data, and the implementation of policies and agreements that define appropriate use of the data. The Steward or his designated representatives are responsible for and authorized to:

- Approve access and formally assign custody of an information technology (IT) resource.
- Specify appropriate controls, based on data classification, to protect the IT resources from unauthorized modification, deletion, or disclosure. The Steward will convey those requirements to administrators for implementation and educate users. Controls shall extend to IT resources outsourced by the university
- Confirm that applicable controls are in place to ensure appropriate level of confidentiality, integrity and availability
- Confirm compliance with applicable controls
- Assign custody of IT resources assets and provide appropriate authority to implement security controls and procedures
- Ensure access rights are re-evaluated when a user's access requirements to the data change (*e.g.*, job assignment change)

Data Administrators are usually system administrators, who are responsible for applying appropriate controls to data based on its classification level and required protection level, and for securely processing, storing, and recovering data. The administrator of IT resources must:

- Implement the controls specified by the Steward(s)
- Provide physical and procedural safeguards for the IT resources
- Assist Stewards in evaluating the overall effectiveness of controls and monitoring
- Implement the monitoring techniques and procedures for detecting, reporting, and investigating incidents

Data Users are individuals who received authorization from the Data Steward to read, enter, or update information. Data Users are responsible for using the resource only for the purpose specified by the Steward, complying with controls established by the Steward, and preventing disclosure of confidential or sensitive information.

4. DATA CLASSIFICATION LEVELS

Confidential Data requires the highest level of privacy and may not be released. Confidential Data is data that is protected by either:

- Legal or regulatory requirements (*e.g.*, HIPAA)
- Contractual agreements (*e.g.*, Non Disclosure Agreements)

See the extended list of Confidential Data for common types of confidential data.

Protected Data must be appropriately protected to ensure a lawful or controlled release (e.g. Connecticut Freedom of Information Act requests). This is all data that is neither **Confidential** or **Public** data (e.g., employee email).

Public Data is open to all users, with no security measures necessary. Data is public if:

- There is either an obligation to make the data public (*e.g.*, Fact Sheets), or
- The information is intended to promote or market the University, or pertains to institutional initiatives (*e.g.*, brochures)

5. CONFIDENTIAL DATA

The University prohibits unauthorized or anonymous electronic or physical access to information technology (IT) resources that store, transmit, or process any of the following:

- University Confidential or Protected Data
- Personally identifiable information (PII)
- Protected health information (PHI) or electronic protected health information (ePHI)
- Credit Card data
- Any other regulated data.

Storage

Confidential Data storage will be limited to the minimum amount, and for the minimum time, required to perform the business function, or as required by law and/or State of Connecticut Data Retention requirements.

University IT resources that are used for storage of Confidential Data shall be clearly marked to indicate they are the property of the University of Connecticut. Servers that store Confidential or Protected Data shall not be used to host other applications or services.

The University prohibits the storage of encrypted or unencrypted Credit Card data in physical or electronic form. Confidential Data may not be stored on personally owned IT resources. Users of portable devices will take extra precautions to ensure the physical possession of the portable device and the protection of the University's Confidential and Protected Data.

The University's Confidential or Private Data may not be accessed, transmitted, or stored using public computers or via email.

System Administrators shall implement access controls on all IT resources that store, transmit, or process Confidential or Protected Data, minimally supporting the requirements defined in the Access Control Policy.

Procedures

Each calendar year, Data Users who are capable of viewing, storing, or transmitting Confidential Data shall complete the Information Security Awareness Training Program.

University employees will perform monthly scans and review results in order to locate and remove PII on each computer under their control. Storage of PII on desktop or laptop computers requires:

1. Explicit permission from the Data Steward,
2. Separate accounts for all users with strong passwords required for all accounts,
3. Whole disk encryption enabled,
4. Security logging and file auditing enabled,
5. Computer firewall enabled and logging,
6. Automatic operating system patching and antivirus software updates,
7. Automatic screen lock after a period of inactivity,
8. Restricted remote access methods, such as remote desktop and file sharing.

Encryption

To maintain its confidentiality, Confidential Data shall be encrypted while in transit across open or insecure communication networks, or when stored on IT resources, whenever possible. Stored data may only be encrypted using approved encryption utilities. To ensure that data is available when needed each department or user of encrypted University data will ensure that encryption keys are adequately protected and that procedures are in place to allow data to be recovered by another authorized University employee. In employing encryption as a privacy tool, users must be aware of, and are expected to comply with, Federal Export Control Regulations.

Activity Logging & Review

IT resources that store, access, or transmit Confidential Data shall automatically log activity into electronic log files. Logging includes system, network, application, database, and file activity, whenever available, and includes creation, access, modification, and deletion activity.

Log files shall be retained electronically for the duration necessary to meet the requirements defined by the State Data Retention schedule S6.

Systems and devices that process, store, or transmit data that are protected by federal regulations (*e.g.*, HIPAA) or by industry requirements (*e.g.*, PCI-DSS) must submit system-generated logs to the Information Security Office's central logging system.

Procedures

System administrators and/or Data Stewards shall examine electronic logs, access reports, and security incident tracking reports, minimally every 30 days, for access control discrepancies, breaches, and policy violations. Log harvesting, parsing and alerting tools can be used to meet these requirements.

Service Providers

Departments shall take steps to ensure that third-party service providers understand the University's Confidential Data Policy and protect University's Confidential Data. No user may give a Third Party access to the University's Protected or Confidential Data or systems that store or process Protected or Confidential Data without a permission from the Data Steward *and* a Confidentiality Agreement in place. Access to these resources must be handled as defined in the University's Access Control Policy.

Physical Security

Each University department that stores, processes, or transmits Confidential Data will maintain a Facility Security Plan that contains the processes necessary to safeguard information technology resources from physical tampering, damage, theft, or unauthorized physical access. Departments will take steps to ensure that all IT resources are protected from reasonable environmental threats and hazards, and opportunities for unauthorized physical access.

Access to areas containing Confidential Data information must be physically restricted. In departments with access to PHI or Credit Card data, all individuals in these areas must wear a University-issued identification badge on their outer garments so that both the picture and information on the badge are clearly visible.

Disposal

Systems administrators will ensure that all data stored on electronic media is permanently destroyed prior to the disposal or transfer of the equipment. The steps taken for the destruction of data will follow the University computer surplus procedures.

Confidential Data maintained in hard copy form will be properly disposed of using University-approved processes when no longer required for business or legal purposes.

Access to areas such as data centers, computer rooms, telephone equipment closets, and network equipment rooms will be restricted to authorized personnel only. Areas where Confidential Data is stored or processed shall be restricted to authorized personnel and access to these areas shall be logged.

6. RISK MANAGEMENT

The Information Security Office (ISO) is responsible for developing a process for conducting Risk Assessments for the University's information technology (IT) resources.

The results of the Risk Assessment will be used to determine security improvements resulting in reasonable and appropriate levels of risk acceptance and compliance for each system.

Results indicating an unacceptable level of risk shall be remediated as soon as possible, as determined by specific circumstances and the timelines decided collectively by the Chief Information Security Officer (CISO), Data Steward, and the Dean, Director or Department Head.

Results of all risk assessments shall be treated as Confidential Data and secured appropriately.

Procedures

Each department is responsible for ensuring that a Risk Assessment is performed biennially for each of the information technology resources in their respective areas. Risk Assessments will also be conducted when there is an environmental or operational change that may affect the security of Confidential Data.

7. SECURITY AWARENESS TRAINING

The University Information Security Office (ISO) maintains an Information Security Awareness Training (ISAT) program that supports the University employees' and students' needs for regular training, supporting reference materials, and reminders to enable them to appropriately protect University information technology resources.

Data Stewards are responsible for ensuring that any user requesting access to Confidential Data has completed the ISAT program before allowing access to that data.

The ISO will provide periodic Information Security reminders and updates, posted on the University Information Security website and using email lists, where appropriate.

Users with access to Confidential Data that is protected under Federal Regulations (*e.g.*, HIPAA, etc.) or by industry standards (*e.g.*, PCI-DSS) must complete the ISAT program annually.

Departments shall maintain appropriate documentation of attendance/completion of the ISAT training where data security training is required by applicable regulatory or industry standards.

8. INCIDENT RESPONSE

The Information Security Office (ISO) will establish, document, and distribute an Incident Response Plan to ensure timely and effective handling of security incidents involving information technology (IT) resources.

University employees with IT responsibilities are responsible for understanding and following the University's Incident Response Plan.

Suspected and confirmed security incidents, their resolution steps, and their outcomes shall be documented by those directly involved. The ISO will ensure that incidents are appropriately logged and archived.

Procedures

All employees must immediately report lost or stolen technology resources to the University Police Department (860-486-4800), the Information Security Office (860-486-8255), and the University's Office of the Controller (860-486-2937).

9. BUSINESS CONTINUITY & DISASTER RECOVERY

Each University department will maintain a current, written and tested Business Continuity Plan (BCP) that addresses the department's response to unexpected events that disrupt normal business (for example, fire, vandalism, system failure, and natural disaster).

The BCP will be an action-based plan that addresses critical systems and data. Analysis of the criticality of systems, applications, and data will be documented in support of the BCP.

Emergency access procedures will be included in the BCP to address the retrieval of critical data during an emergency.

The BCP will include a Disaster Recovery (DR) Plan that addresses maintaining business processes and services in the event of a disaster and the eventual restoration of normal operations. The BCP and DR Plan will contain a documented process for annual review, testing, and revision. Annual testing of the BCP will include desk audits, and should also include tabletop testing, walkthroughs, live simulations, and data restoration procedures, where appropriate. The BCP will include measures necessary to protect Confidential Data during emergency operations.

Data Administrators are responsible for implementing procedures for critical data backup and recovery in support of the BCP. The data procedures will address the recovery point objective and recovery time objectives determined by the Data Steward and other stakeholders.

10. SECURE WEB APPLICATION DEVELOPMENT

Departments will ensure that development, test, and production environments are separated. Confidential Data must not be used in the development or test environments.

All applications must be tested for known security vulnerabilities (such as the OWASP Top Ten) prior to being placed in production and at regular intervals thereafter.

Production application code shall not be modified directly without following an emergency protocol that is developed by the department, approved by the Data Steward, and includes post-emergency testing procedures.

Web servers that host multiple sites may not contain Confidential Data.

All test data and accounts shall be removed prior to systems becoming active in production.

The use of industry-standard encryption for data in transit is required for applications that process, store, or transmit Confidential Data.

Authentication must always be done over encrypted connections. University enterprise Central Authentication Service (CAS), Shibboleth, or Active Directory services must perform authentication for all applications that process, store, or transmit Confidential or Protected Data.

Web application and transaction logging for applications that process, store, or transmit Confidential Data or Regulated Data must submit system-generated logs to the Information Security Office's central logging system.

Departments implementing applications must retain records of security testing performed in accordance with this policy.

Resources

Below is a list of resources that are referenced throughout the information security policies. These resources, templates, and procedures support the information security policies

Reference Information

- OWASP Top Ten
- State of Connecticut Acceptable Use Policy
- State of Connecticut Data Retention schedule S6
- University Information Security Office Website

Procedures and Standards

- Data Destruction Procedures
- Federal Export Control Regulations
- Identity Finder web site
- Incident Response Methodology
- List of Prohibited IT Resources
- Security Patch Guidelines
- University password standards

Resources & Services

- Central Stores Shredding Service
- Online Security Awareness Training
- Security Risk Assessment Tool
- University Centralized Logging Service

Templates and Guides

- Business Continuity Plan Template
- Facility Security Plan
- Sample Confidentiality Agreement

Information Security Glossary

Access Controls: The technology, processes, and procedures used to limit and control access to information technology (IT) resources; these controls are designed to protect against unauthorized entry or use.

Accounts: User accounts are the means of access for real people to a computer system, and provide separation of the users' activities with the system environment, preventing damage to the system or other users. User accounts are assigned a username

Active Directory: A software system that stores, organizes and provides access to information in a directory created by Microsoft. It is responsible for authenticating and authorizing all users and computers within a network.

Administrator: See System Administrator

Authentication: The act of verifying the identity of a user and the user's eligibility to access computerized information.

Authorization: The function of specifying access rights to resources

Availability: The state of a system in a functioning condition

Business Continuity Plan (BCP): A document describing how an organization responds to an event to ensure critical business functions continue without unacceptable delay or change.

CAS: Known as Central Authentication Service, CAS permits a user to access multiple applications while providing their username and password only once.

Chief Information Security Officer (CISO): Head of the Information Security Office

Computer Maintenance: Tasks that must be performed on computers in order to keep them running at optimal efficiency. These tasks include applying security patches, running and maintaining antivirus software, and keeping the computer and data secure.

Confidentiality: Secrecy

Credit Card Data: Data that identifies a credit card account. This data includes primary account numbers (PAN), service codes, expiration date, magnetic stripe or storage chip data, and card validation codes.

Critical Systems And Data: Systems and data that are essential to the operations of the University of to a specific department.

Data: Records and information in a form suitable for use with a computer.

Data Administrators: People who are responsible for applying appropriate controls to data based on its classification level and required protection level. These people are usually system administrators

Data Stewards: People with the responsibility of ensuring the proper handling of administrative, academic, public engagement, or research data.

Data Restoration Procedures: The process used to reinstate data that has been backed up.

Data Users: People that read, enter, or update data.

Desk Audits: The act of reviewing documentation to verify technical and procedural details.

Development Environment: Software staging system, where development takes place, that is separate from the actual system

Disaster: A negative event that lasts longer than the maximum tolerable downtime

Disaster Recovery (DR) Plan: A document that outlines how the University will respond to a disaster and resume critical business functions within a predetermined period of time with minimum amount of loss.

Electronic Protected Health Information (ePHI): Electronic confidential patient information that must be secured against unauthorized exposure as per HIPAA.

Encrypted Data: Data that has undergone the process of encryption

Encryption: A technique used to transform plain text so it is unintelligible but recoverable.

Encryption Key: The input into an encryption algorithm that allows the data to be encrypted.

File Auditing: The logging of opening, modifying, or deleting files on a computer.

File Sharing: Distributing or providing access to electronic data files, usually via a network connection.

Firewall: A network device used to block network access to Information Technology resources

HIPAA: The Health Insurance Portability and Accountability Act address the security and privacy of health data.

Incident: An attempted or successful event resulting in unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operations in an information system.

Information Security: Administrative, physical and technical controls that seek to maintain confidentiality, integrity, and availability of information.

Information Security Awareness Training (ISAT) Program: Training of University faculty and staff regarding the protection of various information technology resources.

Information Security Office (ISO): The unit responsible for overall information security functions for the University.

Information Technology: The act of managing technology, including computer software, information systems, computer hardware, and programming languages.

Information Technology (IT) Resources: Tools that allow access to electronic technological devices, or are an electronic technological device themselves These resources include data; computers and servers; desktop workstations, laptop computers, handheld computing and tracking devices; cellular and office phones; network devices such as data, voice and wireless networks, routers, switches, hubs; and peripheral devices.

Insecure Communication Networks: Data networks that are designed without security requirements in mind.

Integrity: The trustworthiness of information technology resources.

Live simulations: Imitating certain events in order to help test processes and procedures

Log Harvesting: IT resources used to collect logs from various information technology (IT) resources.

Logging: The process of electronically recording activities of IT resources.

Malware: Malicious software designed to disrupt computer operation, gather sensitive information, or gain unauthorized access to information technology (IT) resources.

PCI-DSS: An IT standard for organizations that handle credit card data.

Personally Identifiable Information (PII): Data that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.

Production Environment: Final working stage of software development or network planning when product is rolled out to users.

Protected Health Information (PHI): Confidential patient information that must be secured against unauthorized exposure as per HIPAA.

Public computers: Computers that may be used by anyone in the general public

Recovery Point Objective: The maximum tolerable period in which data might be lost from an IT Service due to a breach or malfunction.

Recovery Time Objective: The duration of time and a service level within which a resource must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in availability.

Regulated Data: Information whose dispersal is determined by permission constraints, some users have access, while others do not.

Remote Desktop: The ability to control the keyboard and mouse of a computer from a remote location.

Risk Assessment: An analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of IT resources.

Security Vulnerability: A security exposure in an operating system or other system software or application software component which an attacker can exploit to gain access to the systems programs or data.

Server: A computer program running to serve the requests of other programs, the “clients".

Screen Lock: An automatic lock of a computer such that it may not be accessed without a username and password

Shibboleth: A method of allowing sites to make informed authorization decisions for individual access of protected online resources in a privacy-preserving manner.

Software Patches: A piece of software designed to fix problems with, or update a computer program or its supporting data

Spam Messages: The use of electronic messaging systems (*e.g.*, email) to send unsolicited bulk messages indiscriminately.

Strong Password: A password that requires extensive resources to guess using either brute force algorithms or human common sense.

System Administrator: A person employed to maintain and operate a computer system or network.

Tabletop Testing: A gathering of relevant individuals to review a specific process in order to improve or update the process.

Test Environment: Staging software development or network construction where the product is stress tested and bug tracked before final deployment.

Third Party: not the original creator of a product.

Threat: An action or event that posses a possible danger to a computer system. The potential for exploitation of a vulnerability.

Unencrypted Data: Plaintext data that has not undergone the encryption process.

Users: People authorized to use information technology (IT) resources.

Virus: Malware that uses it host to propagate itself to other hosts.

Walkthroughs: A simulation of a process via a gathering of individuals in order to test and improve the process.

Whole Disk Encryption: Process by which the entire hard drive of a computer is encrypted.