Information Security Policy Review

2020 / 2021 School Year

The University of Connecticut policies associated with our Information Security program have not been updated for some time. To address this lag between policy updates and with new leadership and team for Information Security, a more holistic approach to security policies was undertaken, resulting in substantial changes to the overall policy, guideline, and standards maintained by Information Security on behalf of the University. The guiding goal of these policy revisions was to streamline and minimize where appropriate the policies in place to improve knowledge and adherence as well as adopt many current best practices (CBP).

Due to the significant changes to the policies, a set of red-lined version changes was not maintained, but this guide is meant to help navigate the changes that were made.

Information Security has reviewed and updated the following policies/standards/guidelines

Name	Comments
Acceptable Use Policy	The Acceptable Use Policy while an update is significantly improved from previous policy which relied heavily on the State of CT Acceptable Use for State Agencies
Data Classification Policy	Significant Changes incorporating several other policies/standards
Data Roles and Responsibilities Policy	Moderate Changes to policy to reflect CBP
Risk Management Policy	Moderate Changes to policy to reflect CBP
Security Awareness Training Policy	Moderate Changes to policy to reflect CBP
Use of the Social Security Number	Minor changes
Vulnerability Management Standard	Significant Changes incorporating several other policies/standards
Network Access Policy	Significant Changes incorporating several other policies/standards (including wireless)
Electronic Logging and Review Standards	Moderate changes to standards
University Password Standard	Previously Updated (2019) - No changes
Incident Response Plan	Previously Updated (2020) - No changes

New Policy/Standard/guideline Created

Name	Comments
System and Application Security Policy	New policy to define expectations around system management
Mobile and Remote Device Security Policy	New policy to better define how/when remote devices should be used
Firewall Policy	New policy to set forth firewall management standards

Policies / Standards / Guidelines planned to be deprecated

Name	Comment
Access Control Policy	Moved to System and Application Security Policy
Data Classification Levels	Moved into Data Classification Policy
Information Security Policy Manual	Redundant - Summary document of all policies and not really needed
Information Security – Wireless Network	Incorporated into Network Access Policy
Information System Activity Review	Moved to System and Application Security Policy
Wireless Access Policy	Incorporated into Network Access Policy
Confidential Electronic Data Security Standard	Moved to Data Classification Policy
Encryption Standard	Moved to Data Classification Policy
Firewall Standard	Changed to a policy
Server Management Standard	Moved to System and Application Security Policy
Extended List of Confidential Data	Moved into Data Classification Policy
List of Prohibited IT Resources	Incorporated into other policies – AUP, SAST
Patch Implementation Guidelines	Incorporated into Vulnerability Management Std
PHP Security Best Practices	No longer accurate - being maintained by other groups
Security Best Practices	Integrated into various other policies/standards
Data Security Checklist	Integrated into various other policies/standards
UConn Higher Education and Opportunity Act	Integrated into AUP
Mobile Device Security Guidelines	Moved to Mobile and Remote Device Security Policy

UCONN

Acceptable Use Policy

Title	Acceptable Use Policy
Policy Owner	Information Technology Services / Chief Information Security Officer
Applies to	This policy applies to all constituents who utilize UConn information technology resources except UConn Health
Campus Applicability	This policy applies to all campuses excluding UConn Health
Effective Date	July 1, 2021
For More Information Contact	UConn Information Security Office
Contact Information	techsupport@uconn.edu or security@uconn.edu
Official Website	https://security.uconn.edu

REASON FOR POLICY

The University's IT resources support many constituencies including students, faculty, staff and guests as well as systems to fulfill the academic, research and administrative needs of the University. These resources must be used in a responsible manner consistent with Federal and State laws and University policies. The purpose of this policy is to define expectations of appropriate use and inform all users of information technology (IT) resources at UConn of their obligation to comply with all existing laws and institutional policies in their use of IT resources.

APPLIES TO

This policy applies to all constituents (students, faculty, staff, affiliates and guests) who utilize UConn's information technology resources including but not limited to, wired and wireless networks, computer based systems and services, printers/copiers, and cloud-based services.

DEFINITIONS (IF APPLICABLE)

Access Point (AP) – A wireless access point is a networking hardware device that allows other Wireless (Wi-Fi) devices to connect to the University network

Information Technology (IT) Resources - includes systems and equipment such as computers, hard drives, printers, scanners, video and audio recorders, cameras, photocopiers and other related devices. Software includes but is not limited to, computer software, including open-source and purchased software and all cloud-based software including infrastructure-based cloud computing and software as a service. Networks include, but are not limited to all voice, video, and data systems, including both wired and wireless network access across the institution.

IoT – Internet of Things are devices that communicate across a network without direct human interaction. These include but are not limited to: Smart assistants, lightbulbs, appliances, and televisions.

POLICY STATEMENT

The appropriate use of UConn IT Resources focuses on three primary areas including: (1) the fair and equitable use of limited resources by all constituents; (2) individual responsibilities in the use of UConn IT resources; and (3) the appropriate use of IT resources in compliance with all applicable federal and state laws, university rules, regulations and policies.

All activities involving the use of UConn IT resources are not personal or private; therefore, users should have no expectation of privacy in the use of these resources. Information stored, created, sent or received via UConn systems including cloud-based systems, may be accessible when required by law, including requests made under the Freedom of Information Act (FOIA), the Family Educational Rights and Privacy Act (FERPA), subpoena, or other legal process, statute, or regulation.

ACCEPTABLE USE

- UConn provides IT resources to enable faculty, students, and staff to accomplish their university-related work and in support of the University's mission. University equipment is to be used primarily in support of the University's mission and may not be used to conduct commercial activities or any activity prohibited by state and federal law or University policy.
- UConn IT Resources may not be used for the illegal download, copying, or distribution of copyright materials without the permission of the copyright owner or where not permitted by fair use standards under the TEACH Act.
- Actions that negatively impact the ability of the University to operate or cause undue stress on IT resources are prohibited. These actions include but are not limited to interfering with the legitimate use of IT resources by others, the introduction of additional software or devices to any IT resource without appropriate authorization, or the mass mailing of unapproved email or other electronic communication.
- Do not intentionally seek or provide information or access to IT resources to which one is not authorized, nor assist others in doing so, nor attempt to subvert or circumvent University systems' security measures nor use University IT resources to subvert of circumvent other systems' security measures for any purpose.
- Do not publish, post, transmit or otherwise make available content that is in violation of law or policy. The University cannot protect individuals against the existence or receipt of material that may be offensive to them. As such, those who make use of electronic communications are warned they may come across or be recipients of material they find offensive or objectionable.
- Do not violate the privacy of other individuals. This includes viewing, monitoring, copying, altering, or destroying any file, data, transmission or communication unless you have been given explicit permission by the owner.
- Do not forge, maliciously disguise or misrepresent your personal identity. This policy does not prohibit users from engaging in anonymous communications, providing that such communications do not otherwise violate the Acceptable Use Policy.

Political Use

- University technology resources may not be used by employees of the University for partisan political purposes or presenting the impression the University has a particular political position except for those individuals authorized by the University as part of their formal responsibilities.

INDIVDIUAL RESPONSIBILITIES

- Protect your data and the institution's data
    - Do not share your password with ANYONE or allow anyone else to use your account(s).
    - Do not use anyone else's account.

    - Be vigilant in identifying and reporting various types of phishing attacks to gain access to your information.
    - Store confidential and/or sensitive data on appropriate University approved services only.
- While UConn owned computers often are maintained and kept up to date by ITS and other University IT organizations, any personally owned devices connecting to the University network (including tablets, cell phones and IoT devices) are expected to be kept up to date with current operating system and software patches, as well as employing appropriate security measures which are automatically updated.
- Do not utilize UConn computing resources, including personally owned computers connected to UConn's network for non-University related commercial activity.
- Users who connect personally owned computers to UConn's network that are used as servers, or who permit others to use their computers, whether directly or through user accounts, have the additional responsibility to respond to any use of their server that is in violation of the Acceptable Use Policy. IT Resource administrators and those who permit the use of the computers by others are responsible for the security and actions of others on their syste ms.

ENFORCEMENT

Violations of this policy may result in appropriate disciplinary measures in accordance with University By-Laws, General Rules of Conduct for All University Employees, applicable collective bargaining agreements, and the Student Code.

Individual or system access may be revoked at any time based on the decision of the Chief Information Security Officer or the Chief Information Officer to protect the confidentiality, integrity, and/or availability of UConn IT Resources.

PROCEDURES/FORMS

Questions about this policy or suspected violations may be reported to any of the following:

Office of University Compliance - https://compliance.uconn.edu (860-486-2530)
Information Technology Services Tech Support - https://techsupport.uconn.edu (860-486-4357)
Information Security Office – https://security.uconn.edu

POLICY HISTORY

Policy created: *05/16/2012*
Revisions: *08/24/2015*
07/01/2020 Revision and update to policy including removing reference to State of Connecticut Acceptable Use Policy and incorporation of new elements

UCONN

Data Classification Policy

Title	Data Classification, Information Technology
Policy Owner	Information Technology Services / Chief Information Security Officer
Applies to	This policy applies to all students, faculty, staff, volunteers, and contractors
Campus Applicability	This policy applies to all campuses except UConn Health
Effective Date	July 1, 2021
For More Information Contact	UConn Information Security Office
Contact Information	techsupport@uconn.edu or security@uconn.edu
Official Website	https://security.uconn.edu

REASON FOR POLICY

This policy defines the classifications of institutional data – i.e., the categories of data that the University is responsible for safeguarding – and the associated measures which are necessary to safeguard each classification. Institutional data commonly exists in many forms including electronic, magnetic, optical, and traditional paper documents. Common types of electronic data includes email messages, spreadsheets, word processing documents, PDF reports, and university managed databases and file storage systems.

APPLIES TO

This policy applies to all University faculty, staff, students, student employees, volunteers, and contractors who have access to protected or confidential information. This policy covers data that is stored, accessed, or transmitted in any and all formats, including electronic, magnetic, optical, paper, or other non-digital formats.

DEFINITIONS (IF APPLICABLE)

Cloud – Any environment not operated by UConn. This includes cloud-based services that provide basic infrastructure including operating system and storage or services that provide a full software stack for an intended purpose or platform offering multiple services.

Confidential Data – Confidential data is institutional information protected by law, government regulations, statutes, industry regulations, contractual obligations, or specific university policies. Examples of confidential data may include Personally Identifiable Information (PII), Protected Health Information (PHI), Educational Records (FERPA), Credit Card Information (PCI-DSS). An extended list of Confidential Data can be found in Appendix A of this policy.

Protected Data – Protected data is institutional information that must be guarded due to proprietary, ethical, privacy, or business process considerations. By default, most administrative data will fall into this classification or if data is not confidential or public.

Public Data – Public data is institutional information that may or must be freely available to the general public. Such information has no local, national, international, or contractual restrictions on access or usage.

POLICY STATEMENT

Through the normal course of business, many individuals at the University of Connecticut collect, maintain, transmit, and/or have access to personal information, financial data, and other information which is protected or confidential in nature. The protection of some types of data is governed by industry or governmental regulations. While other types of information may not be covered by specific legal requirements, it is in the University of Connecticut's best interest to take steps to safeguard all university information reasonably and responsibly.

Except for those classes of data expressly protected by statute, contract, or industry regulation, the data classification examples presented in this policy are guidelines. Ultimate responsibility for the classification in the university environment is determined by the Data Steward and the Office of General Counsel for any given set of data.

Data Protection

The University of Connecticut has established the following requirements/guidelines in order to protect each classification of data.

Public Data

While there are few restrictions on public data, such data should be properly secured to prevent unauthorized modification, unintended use, or inadvertent/improper distribution. It should be understood that any information that is widely disseminated within the university community is potentially available to the public at large.

The following guidelines are for information systems which are used to store and share the University's public data.

- When practical, public data should only be shared via systems over which the University maintains full administrative control, which includes the ability to remove or modify the data in question.
- Information systems such as web servers or cloud services which are used to share public data must be properly secured to prevent the unauthorized modification of published public data.
- Interactive access to databases containing public data such as online directories or library catalogs should be properly secured using query rate limiting, CAPTCHA's or similar technology to impede bulk downloads of entire collections.

Protected Data

Protected data requires additional levels of protection because its unauthorized disclosure, alteration, or destruction could cause damage to the university or its constituents.

In addition to the requirements outlined for public data, protected data must also:

- If stored in the cloud, stored only on cloud-based information systems managed or contracted by the university.

- Protected through the use of authenticated access in order to prevent loss, theft, or unauthorized access, disclosure or modification.
- Printed sensitive data including reports must be stored in a secure manner (file cabinet, closed office, or department where electronic/physical access control systems are in place) when not in use.

Confidential Data

Confidential data (see Appendix A) requires the highest level of protection due to the risk and magnitude of loss or harm that could result from disclosure, alteration, or destruction of the data. Certain types of information (such as health information) may have additional requirements for protection. Wherever possible, confidential information should remain in source systems and not propagated through saved files, spreadsheets, or other file formats. Whenever storage of confidential data is required outside source system it should 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.

In addition to the requirements for Protected data, confidential data must be:

- Protected with strong passwords and should leverage Multi-Factor Authentication whenever such capabilities exist.
- Confidential data should always be stored on devices that have appropriate protection, monitoring and encryption measures in order to protect against theft, unauthorized access and unauthorized disclosure.
- Confidential data may only be transmitted using approved encryption methods.
- Accessed via approved remote access services such as VPN when accessed remotely.
- Confidential data must only be stored on university-owned devices. Confidential data is not permitted to be stored on any personally owned devices including mobile phones, laptops, or home computers.
- The University's Confidential Data may not be accessed, transmitted, or stored using public computers or via email.
- Printed material must be stored only in a locked drawer; a locked room; an area where access is controlled by a guard, cipher lock, and/or card reader; or an area that has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other individuals not on a need-to-know basis.

Encryption

To maintain its confidentiality, data shall be encrypted while in transit across communication networks or when stored. Stored data may only be encrypted using current encryption methodologies. 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.

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 permission from the Data Steward *and* a standard Confidentiality Agreement from University Procurement in place.

Disposal

Systems administrators will ensure that all data stored on electronic media is properly destroyed or wiped to current Department of Defense Data Wipe standards prior to the disposal or transfer of the equipment.

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

ENFORCEMENT

Violations of this policy may result in appropriate disciplinary measures in accordance with University By-Laws, General Rules of Conduct for All University Employees, applicable collective bargaining agreements, and the Student Code.

Questions about this policy or suspected violations may be reported to any of the following:

Office of University Compliance - https://compliance.uconn.edu (860-486-2530)
Information Technology Services Tech Support - https://techsupport.uconn.edu (860-486-4357)
Information Security Office – https://security.uconn.edu

POLICY HISTORY

Policy created: May 16, 2012
Revisions: January 1, 2021 – Reviewed policy and updated for current best practice

APPENDIX A

The following data elements require the highest level of protection. This list may expand based on future regulatory requirements. **This list is not to be construed as a comprehensive list.** Other data may also require similar protections. *Contact your Department's IT Security representative or Information Security Office (Security@uconn.edu) to discuss the security measures that must be implemented for all other data that is not considered public.*

Personally Identifiable Information (PII):

Name (First Name or Initial and Last Name), when stored or displayed with one or more of the following listed data elements:

- Social Security Number
- Driver's License Identifier
- State Identification Card Identifier
- Financial Account Identifiers
- Passport Number
- Alien Registration Number
- Health Insurance Identification
- Biometric Information

Credit Card Information (PCI)

- Primary Account Number (PAN)
- Cardholder Name
- Expiration Date
- Card CVV, CVD, CSC, or CID (3- or 4-digit Card Verification Code)

(Individual) Student University Records (FERPA)

- Grades/Transcripts/Test Scores
- Courses Taken/Scheduled
- Advising Records
- Educational Services Received
- Disciplinary Actions
- Student Financial Aid, Grants, and Loans
- Financial Account and Payment Information (including billing statements, bank account or Credit Card Information)
- Admissions and Recruiting Information (including test scores, high school grade point average, high school class rank)

- Student Personnel Records
- Recording where students are the primary subject (audio or video)

Refer to the University's FERPA policy for additional information.

Personal Health Information

Information that identifies an individual or could reasonably be used to identify the individual in conjunction with a patient's past, present, or future physical or mental health condition including:

- Name, Address, or Telephone Number
- Birthdate
- Medical Record Number
- Admission/discharge Date
- Vehicle ID
- Device ID
- Biometric Identifiers (including facial or fingerprint images)
- Other unique identifying numbers/characteristics/codes

Financial Data

Financial Account Information (including account/routing numbers or Financial Institution Names)

UCONN

Data Roles and Responsibilities Policy

Title	Data Roles and Responsibilities Policy, Information Technology
Policy Owner	Information Technology Services / Chief Information Security Officer
Applies to	This policy applies to all students, faculty, and staff
Campus Applicability	This policy applies to all campuses except UConn Health
Effective Date	July 1, 2021
For More Information Contact	UConn Information Security Office
Contact Information	techsupport@uconn.edu or security@uconn.edu
Official Website	https://security.uconn.edu

REASON FOR POLICY

This policy defines the responsibilities of individuals within the organization in protecting the University of Connecticut's data assets.

APPLIES TO

This policy applies to all University faculty, staff, students, student employees, volunteers, and contractors who have access to or have been assigned one of the roles defined in this policy.

DEFINITIONS (IF APPLICABLE)

POLICY STATEMENT

Through the normal course of operations of the university, ever increasing amounts of data are created, processed, modified, and eventually disposed of as part of daily activities. To ensure the proper management of the various data sets, the university has defined the following roles and responsibilities to ensure data is properly protected, used, and managed throughout its lifecycle.

Data Stewards are employees of the university responsible for the overall use and proper handling of administrative, academic, public engagement, or research data. Data Stewards are responsible for classifying data according to the University's Data Classification Policy, ensuring that appropriate steps are taken to protect data, and the implementation of policies and agreements that define appropriate use of data.

The Data Steward or their designated representatives are responsible for:

- Ensuring the accuracy of the information they are responsible for is accurate
- Authorizing the specific use of information across the organization
- Working with other Data Stewards to resolve conflicting data issues
- Specify appropriate controls, based on data classification, to protect the data from unauthorized modification, deletion, or disclosure
- Ensuring access rights are evaluated on a regular basis

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

also responsible for securely processing, storing and recovering data. The Data Administrator is accountable for:

- Implementing the appropriate controls specified by the Data Stewards
- Removal of access rights to specific data resources due to a job change or separation from the University
- Implementing the appropriate monitoring techniques and procedures for detecting, reporting, and investigating incidents
- Assist Data Stewards in evaluating the overall effectiveness of controls and monitoring

Data Users are individuals who receive authorization from the Data Steward/Administrator to access, enter, or update information. Data Users are responsible for using the resource only for the purpose specified by the Data Steward, complying with controls established by the Steward, and preventing disclosure or confidential or protected information.

ENFORCEMENT

Violations of this policy may result in appropriate disciplinary measures in accordance with University By-Laws, General Rules of Conduct for All University Employees, applicable bargaining agreements, and the Student Code.

Questions about this policy or suspected violations may be reported to any of the following:

Office of University Compliance - https://compliance.uconn.edu (860-486-2530)
Information Technology Services Tech Support - https://techsupport.uconn.edu (860-486-4357)
Information Security Office – https://security.uconn.edu

POLICY HISTORY

Policy created: May 16, 2012
Revisions: January 1, 2021 – Reviewed policy and updated for current best practice

UCONN

IT Risk Management Policy

Title	Risk Management, Information Technology
Policy Owner	Information Technology Services / Chief Information Security Officer
Applies to	This policy applies to all faculty, staff, student employees, and volunteers
Campus Applicability	This policy applies to all campuses except UConn Health
Effective Date	July 1, 2021
For More Information	UConn Information Security Office
Contact Information	techsupport@uconn.edu or security@uconn.edu
Official Website	https://security.uconn.edu

REASON FOR POLICY

The University environment is constantly changing from both a capability and use of technology perspective, as well as threats against these technologies. To provide the highest level of protection for the university, department and system owners are responsible for regular assessments of risks to their technology platforms. The Information Security Office is responsible for overseeing the evaluation of IT risk across the organization.

APPLIES TO

This policy applies to all University faculty, staff, student employees, and volunteers who regularly interact with or have access to confidential or protected information within the university.

DEFINITIONS (IF APPLICABLE)

Confidential Data – Confidential data is institutional information protected by law, government regulations, statutes, industry regulations, contractual obligations, or specific university policies. Examples of confidential data may include Personally Identifiable Information (PII), Protected Health Information (PHI), Educational Records (FERPA), Credit Card Information (PCI-DSS). An extended list of Confidential Data can be found in Appendix A of this policy.

Protected Data – Protected data is institutional information that must be guarded due to proprietary, ethical, privacy, or business process considerations. By default, most administrative data will fall into this classification or if data is not confidential or public, it will fall into the protected data category.

POLICY STATEMENT

Due to the size and complexity of the UConn environment, each department and system owner is responsible for conducting a regular and ongoing risk assessment of the Information Technologies they are responsible for overseeing.

In conducting a risk assessment, departments/individuals should evaluate risks to Information Technology based on a People, Process, Technology (PPT) methodology. Using this methodology and leveraging ISO policies including the Acceptable Use Policy, Confidential Data Policy, Data Roles and Responsibilities Policy, Security Awareness Training Policy and System and Application Security Policy (available at https://security.uconn.edu) to evaluate opportunities to reduce risk to the confidentiality, integrity and availability of information technology assets.

Some organizations will be required to do regular risk assessments as a regulatory or industry requirement. Organizations typically focusing on Personal Health Information or Credit Card Processing will have more formal risk assessments conducted by their leadership and review by Information Security Office on an annual basis.

ENFORCEMENT

Violations of this policy may result in appropriate disciplinary measures in accordance with University By-Laws, General Rules of Conduct for All University Employees, applicable bargaining agreements, and the Student Code.

Questions about this policy or suspected violations may be reported to any of the following:

Office of University Compliance - https://compliance.uconn.edu (860-486-2530)
Information Technology Services Tech Support - https://techsupport.uconn.edu (860-486-4357)
Information Security Office – https://security.uconn.edu

POLICY HISTORY

Policy created: May 16, 2012
Revisions: January 1, 2021 – Reviewed policy and updated for current best practice

UCONN

Security Awareness Training Policy

Title	Security Awareness Training Policy, Information Technology
Policy Owner	Information Technology Services / Chief Information Security Officer
Applies to	This policy applies to all faculty, staff, student employees, and volunteers
Campus Applicability	This policy applies to all campuses except UConn Health
Effective Date	July 1, 2021
For More Information Contact	UConn Information Security Office
Contact Information	techsupport@uconn.edu or security@uconn.edu
Official Website	https://security.uconn.edu

REASON FOR POLICY

The Information Security Office maintains an active Security Awareness Training program available to all faculty, staff, and student employees. This policy outlines the expectations for individuals and departments in assisting with ensuring the confidentiality, integrity, and availability of university systems, services, and data.

APPLIES TO

This policy applies to all University faculty, staff, student employees, and volunteers who regularly interact with or have access to confidential or protected information within the university.

DEFINITIONS (IF APPLICABLE)

POLICY STATEMENT

While the Information Security Office maintains an active information security program, individual faculty and staff knowledge of the threats and risks to the University's systems and data is a critical component in helping to defend the University from attack.

The University Information Security Office (ISO) maintains an Information Security Awareness program that supports University employees' and students' needs for regular training. Training on important information security topics is available or communicated in multiple ways including:

- Online training systems with a variety of topics relevant to Information Security (available at https://security.uconn.edu/training)
- Communications to targeted groups by email of ongoing or imminent threats
- Postings on various web-based systems across the university (security.uconn.edu or techsupport.uconn.edu)
- Availability of ISO staff for in person discussions on information security

As part of their ongoing operations and employee development all departments (Academic and Administrative) should identify opportunities to engage faculty, staff, and student employees in Security Awareness training annually. These opportunities may include those offerings from the Information Security Office or a tailored program for specific threats against departments or systems which may also be included in procedural manuals or scheduled as group training opportunities.

In some areas, Security Awareness training may be mandatory based on federal or industry regulations. Training for these programs must be coordinated with the Information Security Office to ensure regulatory requirements are met.

ENFORCEMENT

Violations of this policy may result in appropriate disciplinary measures in accordance with University By-Laws, General Rules of Conduct for All University Employees, applicable bargaining agreements, and the Student Code.

Questions about this policy or suspected violations may be reported to any of the following:

Office of University Compliance - https://compliance.uconn.edu (860-486-2530)
Information Technology Services Tech Support - https://techsupport.uconn.edu (860-486-4357)
Information Security Office – https://security.uconn.edu

POLICY HISTORY

Policy created: May 16, 2012
Revisions: January 1, 2021 – Reviewed policy and updated for current best practice

UCONN

Information Technology Confidential Data Policy

Title	Use of the Social Security Number
Policy Owner	Information Technology Services / Chief Information Security Officer
Applies to	This policy applies to all students, faculty, and staff
Campus Applicability	This policy applies to all campuses except UConn Health
Effective Date	July 1, 2021
For More Information Contact	UConn Information Security Office
Contact Information	techsupport@uconn.edu or security@uconn.edu
Official Website	https://security.uconn.edu

REASON FOR POLICY

Social Security numbers have been used to uniquely identify students and employees in various University systems. As systems are updated and replaced, the reliance on Social Security numbers should be used only as required.

APPLIES TO

This policy applies to all University faculty, staff, students, student employees, volunteers, and contractors who have access to or have been assigned one of the roles defined in this policy

DEFINITIONS (IF APPLICABLE)

POLICY STATEMENT

The purpose of this policy is to protect the confidentiality and privacy of students and employees of the University of Connecticut and to ensure that steps are taken concerning the collection, use and disclosure of Social Security numbers.

In order to protect the Social Security number of its students, staff, faculty and affiliates, the University of Connecticut will:

1. Discontinue the collection of Social Security numbers except where necessary for employment records, financial aid records, and other business and governmental transactions as required by law or to satisfy a business requirement when permitted by law.
2. Develop a University of Connecticut identifier to be assigned to all students, faculty, staff and other individuals associated with the University, to uniquely and permanently identify the individual. This identifier will be considered public information and be assigned and distributed to the individual upon initial association with the University. It will be used in all electronic and paper data systems to identify, track and service the individual.
3. Ensure that no new systems or technology will be purchased or developed by the University of Connecticut that use the Social Security number as its primary key to the database except where required by law. Any exemption to this policy must be approved by University Compliance.
4. Ensure that new systems or technologies purchased or developed by the University of Connecticut will use Social Security numbers as data elements only (not as keys to databases)

when required by law or business necessity. Approval by the Council of Data Stewards is required for inclusion of the Social Security number in databases.

5. Ensure that all requests (verbal or written) for which faculty, staff or students are **required** to provide their Social Security number contain or have appended to them a statement explaining the University's request; e.g., the legal obligation on which the request is based, if there is one and the use that will be made of the Social Security Number.
6. Ensure that all requests (verbal or written) for which faculty, staff or students are **requested to voluntarily** provide their Social Security number contain or have appended to them a statement explaining the University request and its purpose. The statement must indicate that no service or privilege will be withheld upon failure to provide the Social Security number and that the person may use the identifier provided by the University of Connecticut in place of the Social Security number.
7. Ensure that any request for any form or document that contains the Social Security number, where the Social Security number is not the primary reason for the request, be accompanied by a statement indicating that the Social Security number is not required and should be blanked out on the form or document prior to being provided.
8. Ensure that no new systems purchased or developed by the University of Connecticut display Social Security number visually, whether on computer monitors or on printed forms or other output, unless required by law.
9. Access to Social Security Numbers in online systems must be restricted as appropriate and visible only for required or approved uses.

ENFORCEMENT

Violations of this policy may result in appropriate disciplinary measures in accordance with University By-Laws, General Rules of Conduct for All University Employees, applicable collective bargaining agreements, and the Student Code.

Questions about this policy or suspected violations may be reported to any of the following:

Office of University Compliance - https://compliance.uconn.edu (860-486-2530)
Information Technology Services Tech Support - https://techsupport.uconn.edu (860-486-4357)
Information Security Office – https://security.uconn.edu

POLICY HISTORY

Policy created: September 24, 2020
Revisions:

UConn Systems and Application Vulnerability Management Standards

Purpose

The purpose of the Server Vulnerability Management Standards is to establish the expectations and guidelines for applying service packs, hotfixes, and security patches (referred to generally as "security patches" throughout this document). In the interest of reducing the University's vulnerability exposure.

Definitions

Security patch – Code that will update the current version of a script or software, often used to fix a bug, update security, or add a new feature or new functionality (includes service packs, hotfixes, etc.).
Severity – This is the level of importance of the security patch as defined by the vendor or as a Common Vulnerability Scoring System (CVSS) score.
Priority – This is the level of importance of the security patch as defined by UConn. This includes a timeframe for the expected installation of the security patch.
Data - Information collected, stored, transferred, or reported for any purpose in digital format. Data can include: financial transactions, lists, identifying information about people, projects or processes, and information in the form of reports. Because data has value and because it has various sensitivity classifications defined by federal law and state statute, it must be protected.

ISO – Information Security Office

CISO – Chief Information Security Officer.

Scope

All systems and applications operated by or on behalf of the University. This includes Operating Systems, Middleware (Java, Adobe, etc.) and applications both on-premise and in the cloud. While this document focuses primarily on security and bug patching, it is necessary to keep all software up to date and on supported code to prevent situations where multiple upgrades need to occur, or software is no longer supported.

Introduction

Security patches are updates to products to resolve a known issue or provide a workaround. Service packs update systems to the most current code base. Being on the current code base is important because that's where the operating system support focuses on fixing problems. Individual hotfixes and security patches should be adopted on a case-by-case, "as-needed" basis. They may or may not be relevant to an installation. Evaluate the update, assess the risk of applying or not, and apply if appropriate.

The basic rules are:

The risk of implementing the service pack, hotfix, or security patch should ALWAYS be LESS than the risk of not implementing it.

And,

By implementing a security patch, the system should never be worse. If unsure, then take steps to ensure that there is no doubt before moving changes into production.

Scheduling and Delivery

General system updates, service packs, or hotfixes should be installed at a time that limits interference with the majority of users. Where appropriate testing and signoff have occurred as part of the University change control process, general upgrades may occur at any time convenient to the user base and system administrator or where available on a regularly scheduled process.

Security patches, which may also be included in regular system updates, service packs, or hotfixes should be applied as soon as feasibly possible (following research, testing notification) using the following timeframes:

CVSS or Vendor Defined Criticality	Timeline
CVSS (9.0 – 10.0) or Critical designation by vendor	Patches should be installed as soon as reasonably possible or mitigating controls put in place to reduce vulnerability. Patch Timeframe – Within 7 days Mitigation Timeframe – Within 2 days (if necessary)
CVSS (7.0 – 8.9) or High designation by vendor	Patches should be installed as soon as reasonably possible or mitigating controls put in place to reduce vulnerability. Patch Timeframe – Within 14 days Mitigation Timeframe – Within 2 days (if necessary)
CVSS (4.0 – 6.9) or Medium designation by vendor	Remediated or accepted and documented in Nessus within 30 days
CVSS (0.1 – 3.9) or Low designation by vendor	Remediated or accepted and documented in Nessus within 60 days

Exceptions

If the application of security patches is not feasible, mitigating controls must be identified and implemented. The mitigating control(s) selected should be in proportion to the risk. If mitigating controls cannot be implemented, then a risk exception must be documented in Tenable and reviewed by the Information Security Office / ITS Risk Council. Mitigating controls or risk exceptions are to be used for limited periods of time and may not exceed one year without approval of the Chief Information Security Officer.

Responsibilities and Practices of the Information Security Office (ISO)

The ISO conducts scans of the University network resources to identify vulnerabilities. Only ISO or units approved by the Chief Information Security Officer may conduct such scans. The ISO will create dashboards and ensure access is available to all technology staff managing servers or applications, as appropriate.

Vulnerability Response Process and Responsibilities

The Information Security Office maintains the Tenable vulnerability scanning service and regularly scans areas of the network where servers and applications are known to exist (server farm network). Results of scans are immediately available via individuals created custom reports for systems of interest. Individuals responsible for systems and applications are responsible for setting up and monitoring these reports or manually checking in on a regular basis.

Once notified of the vulnerable resource, the IT administrator or third party managing that resource should follow the schedule presented in the "Scheduling and Delivery" section to close the vulnerability. Care should be taken to ensure all actions are taken to address the vulnerability or it may continue to be a risk or falsely reported as a risk. If a risk is accepted, this should be documented in Tenable within the remediation timeframe.

If the vulnerability is not remediated in the recommended or agreed upon timeframe and no exception has been granted, ISO staff may take necessary actions to safeguard the University network, including disconnecting the resource from the network to protect other computers and the integrity of the University computing environment.

UConn Electronic Data Logging Standard

Purpose

Logging is an essential information security control that is used to identify, respond, and prevent operational problems, security incidents, policy violations, fraudulent activity. It assists in business recovery activities and, in many cases, comply with federal, state, and local laws and regulations. The purpose of the Logging Standard is to define logging expectations and requirements regarding University of Connecticut's (UConn) electronic log data collection and analysis.

Underlying Requirements

All systems that handle confidential or protected information, accept network connections, or make access control (authentication and authorization) decisions shall record and retain audit-logging information sufficient that review the following:

1. A time and date entry recording when the event or action has taken place
2. The activity or action was performed
3. Who or what performed the activity or action, including where or on what system the activity was performed from (subject) If at all possible, an IP address should be captured at the time of writing the event
4. The activity or action was performed on (object)
5. Tool(s) the activity was performed with
6. The status (such as success vs. failure), outcome, or result of the activity

Activities to be Logged

Therefore, logs shall be created whenever any of the following activities are requested to be performed by the system:

1. Create, read, update, or delete confidential information, including confidential authentication information such as passwords
2. Create, update, or delete information not covered in #1
3. Initiate a network connection
4. Accept a network connection
5. User authentication and authorization for activities covered in #1 or #2 such as user login and logout
6. Grant, modify, or revoke access rights, including adding a new user or group, changing user privilege levels, changing file permissions, changing database object permissions, changing firewall rules, and user password changes

7. System, network, or services configuration changes, including installation of software patches and updates, or other installed software changes
8. Application process startup, shutdown, or restart
9. Application process abort, failure, or abnormal end, especially due to resource exhaustion or reaching a resource limit or threshold (such as for CPU, memory, network connections, network bandwidth, disk space, or other resources), the failure of network services such as DHCP or DNS, or hardware fault
10. Detection of suspicious/malicious activity such as from an Intrusion Detection or Prevention System (IDS/IPS), anti-virus system, or anti-spyware system

Logging additional items may be deemed necessary for higher risk or business critical systems at the discretion of the System Administrator and Information Security Office.

Elements of the Log

Such logs shall identify or contain at least the following elements, directly or indirectly. In this context, the term "indirectly" means unambiguously inferred.

1. Time and Date: It is recommended that the logging method leverage RFC 3339, ISO 8601 or UNIX Timestamps as a method to record the date and time the event took place.
2. Type of action – examples include authorize, create, read, update, delete, and accept network connection.
3. Subsystems performing the action – examples include process or transaction name, process or transaction identifier.
4. Identifiers (as many as available) for the subject requesting the action – examples include user name, computer name, IP address, and MAC address (Note that such identifiers should be standardized in order to facilitate log correlation).
5. Identifiers (as many as available) for the object the action was performed on – examples include file names accessed, unique identifiers of records accessed in a database, query parameters used to determine records accessed in a database, computer name, IP address, and MAC address. (Note that such identifiers should be standardized in order to facilitate log correlation.)
6. Before and after values when action involves updating a data element, if feasible.
7. Whether the action was allowed or denied by access-control mechanisms.
8. Description and/or reason-codes of why the action was denied by the access-control mechanism, if applicable.

Formatting and Storage

The system shall support the formatting and storage of audit logs in such a way as to ensure the integrity of the logs and to support enterprise-level analysis and reporting. Mechanisms known to support these goals include, but are not limited to, the following:

1. Microsoft Windows Event Logs collected by a centralized log management system;
2. Logs in a well-documented format sent via syslog, syslog-ng, or syslog-reliable network protocols to a centralized log management system;

3. Logs stored in an ANSI-SQL database that itself generates audit logs in compliance with the requirements of this document; and

4. Other open logging mechanisms supporting the above requirements including those based on CheckPoint OpSec, ArcSight CEF, and IDMEF.

Whenever possible, the logs should be forwarded to the university's ITS Managed SIEM (Security Information and Event Management instance that is managed by the Information Security Office.

Required Logging Practices

- Systems should be time-synchronized via a network time source (preferably time.uconn.edu). If possible, log events should include an indication of time zone.
- Log data must be transmitted securely via an encrypted mechanism when possible to preserve integrity and confidentiality. This could include encrypting data prior to transmission or providing an encrypted tunneling mechanism. (Compliance can be achieved several ways – contact the Information Security Office if you need assistance or to assure you are forwarding your logs to the University Central Log Repository).
- When possible, audit the access to and modification of log data.
- All administrator or root access and operations must be logged (including read-only administrator access).
- Log data should be housed centrally (unless isolation is dictated for compliance reasons), and robust role-based access controls should be utilized for data analysis and retrieval.
- Alarms raised by University IT resources (e.g., console alerts or messages; system log exceptions; network management alarms; alarms raised by access control systems) must be logged and retained for a specified period.
- Activation/deactivation of protection systems such as anti-virus, intrusion detection, and file integrity systems must be logged.
- The following data must never be included in University server log data:
    - Social Security Numbers
    - Clear text authentication credentials (e.g., passwords)
    - PII or financial information (e.g., financial account numbers, credit card numbers, etc.)
- Timestamps should be recorded in RFC3339 or ISO-8601 format, whenever possible:
    - Minimally : 2013-04-03
    - Acceptable: 2013-04-03 23:45
    - Ideally: 2020-12-09T16:09:53+00:00 (in UTC)
    - UTC is preferred to work around possible issues with Daylight Saving Time.

(This is critical data that assists when investigating the timeline of an incident.)

- Logging facilities and log information should be protected against tampering, modification, destruction, and unauthorized access. Where possible, system administrators should not have permission to erase, deactivate, or modify logs of their own activities.
- Windows servers must maintain a copy of log data external to the server generating the log data to prevent tampering in the case of virus, malware or other security event.

Log Reviews

Logs should be reviewed at least on a monthly basis. Logs must be reviewed within a 24-hour period in response to suspected or reported security problems on systems containing confidential data or as requested by the Information Security Office. Automated tools in place of manual log reviews are preferable as long as proper alerts or reports are generated and acted upon.

Data Stewards are responsible for determining which systems require scheduled log review.

Log review shall include investigation of suspicious activity, including escalation to the Information Security Office or the campus incident response process as appropriate.

Individuals shall not be assigned to be the sole reviewers of their own activity.

Log Retention Schedules

The retention schedule applied for log data depends heavily upon the policies, regulations, and/or standards that govern the type of data recorded in log events (and/or the purpose of the systems of origin). Data not governed by any other consideration should be interpreted as subject to Schedule S6 as appropriate, allowing system administrator and/or data steward discretion in selecting a log retention period. However, when data is governed by other regulations/standards, the strictest common denominator for retention requirements should be selected.

UCONN

System and Application Security Policy

Title	System and Application Security Policy
Policy Owner	Information Technology Services / Chief Information Security Officer
Applies to	This policy applies to all students, faculty, and staff
Campus Applicability	This policy applies to all campuses except UConn Health
Effective Date	July 1, 2021
For More Information Contact	UConn Information Security Office
Contact Information	techsupport@uconn.edu or security@uconn.edu
Official Website	https://security.uconn.edu

REASON FOR POLICY

The proper maintenance and oversight of systems and applications used by university constituents is an important requirement for ensuring the security of university data.

APPLIES TO

This policy applies to all individuals responsible for operating or overseeing any University system or application whether on premise or in the cloud.

DEFINITIONS (IF APPLICABLE)

ITS – Information Technology Services

SaaS – Cloud-based service that is delivered via the web based on either a monthly or annual subscription

PaaS – Cloud-based service that provides a platform allowing for the development of software using an established framework to improve development time and management of cloud services

PII (Personally Identifiable Information) – Information that either singularly or in conjunction with other data elements could reasonably lead to the identification of specific individuals

POLICY STATEMENT

The proper maintenance and review of systems and applications is critical to protecting the data they store or process. While requirements may vary as to the administration and operation of any system or application, the following are required of any individual responsible for a system or application related to the University of Connecticut computing environment whether on-premise or in the cloud.

System Ownership

All systems supporting any aspect of the university must have an identified owner and responsible party for ensuring the controls specified in this document. Where a system is fully cloud-based, a UConn faculty or staff member must be identified who is responsible for overseeing the following controls are appropriately applied and adhered to by the cloud provider.

System and Application Security

All software and services used to process University of Connecticut information are subject to an Information Security review and sign off prior to their purchase or development. Information Security reviews will evaluate specific risks and controls available and necessary based on the information being

processed. The system owner will be responsible for the deployment of the agreed upon security controls prior to enabling the production capability of the system or application.

Only necessary software should be loaded on systems, and old versions of software removed. The use of web browsers should be limited to the management of the system only.

System Access
Access to information in the possession of or under the control of the University of Connecticut must be provided on a need-to-know basis. Information must be disclosed only to individuals who have a legitimate and approved business need for information. Information may only be used for its intended purpose and other uses of university information without the approval of the data owner is not allowed.

Patching and Maintenance
All individuals (including faculty, staff, or students) who have taken on or been assigned the responsibility of managing any system or application attached to the University of Connecticut network or any cloud system that holds a relationship to the University of Connecticut or holds University of Connecticut data, must ensure the timely implementation of operating systems and application patches to provide for the confidentiality, integrity, and availability of said systems or data. The ongoing maintenance of applications and the application of software updates is an activity that should be regularly scheduled on a minimum quarterly basis. ITS and many other parts of the University maintain systems to simplify the patching of operating systems.

Cloud-based SaaS and PaaS systems typically remove the requirement for patching and maintenance, as the responsibility for this is handled by the vendor.

User Management
University of Connecticut ITS provides a centralized user identity and access management that supports identity validation and access management (IAM) using a NetID and password. Systems and applications that rely on the University IAM platform for authenticating individual access rights can forgo the need for user management outside that of assigning any roles within the system or application, as necessary.

Systems and Applications that do not use the central IAM solution must have a written plan and responsible individual for the creation, modification, and deletion of user ID's at time of separation from the University for faculty/staff or on at least an annual basis for students. This includes a process for ensuring the secure creation of passwords and a secure password reset process for validating an individual's identity prior to resetting the password.

Systems where individuals have access to a significant amount of the PII of other constituents (including students, faculty, staff, alumni, and vendors) or significant amounts of regulated data should leverage multi-factor authentication wherever possible.

Auditing of Systems and Application Logs
System and application logs should be reviewed for inappropriate access on a regular basis (at least monthly) or via automated systems capable of detecting misuse through the analysis of frequent password failures, geographic anomalies, or inappropriate access attempts. ITS maintains a centralized logging and reporting platform which can assist in the analysis of large amounts of data often associated with system and application logs.

System and Application Lifecycle Management
Any system or application that is no longer supported by the vendor or is replaced by newer technology should be decommissioned as soon as possible. The proper update of systems and applications is critical to protecting the confidentiality, integrity and availability of the system/application and its data. The decommissioning process must include the proper retirement of any physical hardware or virtual images and the proper destruction of any media (hard drives, tapes, etc.) that may have data. Cloud services

that are decommissioned should ensure the proper handling of any data (return and/or destruction) in the cloud vendors possession as part of the contract cancellation.

Protection of Regulated Data
Certain classes of information stored within University of Connecticut systems and applications have additional regulatory requirements associated with their storage and/or transmission. This data includes but is not limited to: PII (Personally Identifiable Information) including certain combinations of data regarded as sensitive PII; PHI (Personal Health Information), PCI (Payment Card Industry) information or FERPA (Family Educational Rights and Privacy Act). Other agencies or organizations may also contractually require additional protections of information or datasets which also must be adhered to.

Mandatory Reporting
All suspected policy violations, system intrusions, and other conditions that might jeopardize University of Connecticut information or information systems must be immediately reported to the Information Security Office.

ENFORCEMENT

Systems and applications that do not follow the standards set forth in this policy may be administratively shut down or access restricted to on campus or individual personnel only. Systems maintained at the departmental or individual level may incur costs in association with enabling the proper protections or in the event of a data exposure.

Violations of this policy may result in appropriate disciplinary measures in accordance with University By-Laws, General Rules of Conduct for All University Employees, applicable collective bargaining agreements, and the Student Code.

PROCEDURES/FORMS

Questions about this policy or suspected violations may be reported to any of the following:

Office of University Compliance - https://compliance.uconn.edu (860-486-2530)
Information Technology Services Tech Support - https://techsupport.uconn.edu (860-486-4357)
Information Security Office – https://security.uconn.edu

POLICY HISTORY

Policy created: September 24, 2020
Revisions:

UCONN

Mobile and Remote Device Security Policy

Title	Mobile and Remote Device Security, Information Technology
Policy Owner	Information Technology Services / Chief Information Security Officer
Applies to	This policy applies to all faculty, staff, student employees, and volunteers
Campus Applicability	This policy applies to all campuses except UConn Health
Effective Date	July 1, 2021
For More Information Contact	UConn Information Security Office
Contact Information	techsupport@uconn.edu or security@uconn.edu
Official Website	https://security.uconn.edu

REASON FOR POLICY

Mobile and remote devices are important tools for the University, and their use is supported to advance the mission of the university. Mobile and remote devices also represent a significant risk to information and data security. If appropriate security measures and procedures are not applied, mobile and remote devices can serve as a conduit for unauthorized access to University data and IT Resources that can subsequently lead to data leakage and a path for compromise of other systems.

APPLIES TO

This policy applies to all University faculty, staff, student employees, and volunteers who use mobile or remote devices to access any non-public IT Resources owned or managed by the University.

DEFINITIONS (IF APPLICABLE)

IT Resources – includes systems and equipment such as computers, hard drives, printers, scanners, video and audio recorders, cameras, photocopiers and other related devices. Software includes but is not limited to, computer software, including open-source and purchased software and all cloud-based software including infrastructure-based cloud computing and software as a service. Networks include, but are not limited to all voice, video, and data systems, including both wired and wireless network access across the institution.

Mobile Electronic Device – Laptop, cellular phone, or other mobile device such as a tablet, USB drives or CD/DVD media

Remote Device – Personal computer used in a private residence

POLICY STATEMENT

University of Connecticut faculty, staff, student employees, and volunteers who use mobile or remote devices are responsible for any institutional data which is stored, processed and/or transmitted via a mobile or remote device and for following the security requirements set forth in this policy.

To adequately protect the data and information systems of the University, all individuals covered under this policy are expected to meet the following requirements:

All users of a mobile electronic device used to access non-public university systems must make take the following measures to secure the device:

- Configure the device to require a password (minimum of 10 characters), biometric identifier, PIN (minimum of 6 characters) or swipe gesture (minimum of 6 swipes) to be entered before access to the device is granted. Device must automatically lock and require one of the authentication methods after no more than 5 minutes of idle time.
- Maintain device Operating System and patch levels to currently supported versions.
- Enable the device's remote wipe feature to permit a lost or stolen device to be securely erased.
- Securely store at all times electronic devices to minimize loss via theft or accidental misplacement.

Wherever practical, elements of these requirements will be enforced via centrally administered technology controls.

STORAGE OF CONFIDENTIAL DATA

In general, confidential data should not be stored on mobile devices (including laptops), however, in certain instances depending on job responsibilities, this may be unavoidable. In these instances, confidential data must be stored on University owned devices ONLY with the following requirements:

- Except when being actively used, confidential information must at all times be encrypted on any device through a mechanism approved by the University. Alternatively, whole drive encryption software may be deployed to meet this requirement.
- Mobile devices must have University supported software enabled and running to identify, protect, and respond to any threats to the data or operating systems of the devices.
- Device must have Mobile Device Management software installed to facilitate devices protection including remote wipe and device location technology for recovery if possible.

DEVICE DECOMISSION OR SEPARATION FROM UNIVERSITY

When mobile devices, specifically personally owned devices which may have had access to University resources or data that are no longer used, donated, or given to anyone, it is the responsibility of the device owner to ensure any University information is securely deleted from the device, including University related e-mails/accounts, User ID and Password, or other cached credentials use to access University systems.

In the event of separation from the University, it is the employee's responsibility to delete any University related e-mail accounts or University licensed software that may have been installed on personal devices or computers.

ENFORCEMENT

Violations of this policy may result in appropriate disciplinary measures in accordance with University By-Laws, General Rules of Conduct for All University Employees, applicable bargaining agreements, and the Student Code.

Questions about this policy or suspected violations may be reported to any of the following:

Office of University Compliance - https://compliance.uconn.edu (860-486-2530)
Information Technology Services Tech Support - https://techsupport.uconn.edu (860-486-4357)
Information Security Office – https://security.uconn.edu

POLICY HISTORY
Policy created: January 1, 2021
Revisions:

UCONN

Firewall Policy

Title	Firewall Policy
Policy Owner	Information Technology Services / Chief Information Security Officer
Applies to	This policy applies to all students, faculty, and staff
Campus Applicability	This policy applies to all campuses except UConn Health
Effective Date	July 1, 2021
For More Information Contact	UConn Information Security Office
Contact Information	techsupport@uconn.edu or security@uconn.edu
Official Website	https://security.uconn.edu

REASON FOR POLICY

Firewalls provide a valuable protection and detection capability for the organization when properly configured, managed, and monitored. Ensuring a common set of configurations across the organization is critical to maximizing their capabilities to protect the organization and in support of the security of the University.

APPLIES TO

This policy applies to all University faculty, staff, students, student employees, volunteers, and contractors who have responsibility for controlling or configuring firewalls

DEFINITIONS (IF APPLICABLE)

EOL – End of Life
EOS – End of Support
IANA – Internet Assigned Numbers Authority (iana.org)

POLICY STATEMENT

The University operates in a highly flexible and adaptive security environment to meet its academic, research, and administrative missions. While the ability to adapt to meet the ever-changing needs of the University are important, oversight and reporting of firewall activities are critical to the successful protection and operation of the University environment.

Firewall Configuration Standards

- All firewalls must be properly maintained from a hardware and software perspective. This includes proper lifecycle planning for EOL and EOS software/hardware and regular review (annually) of firewall rulesets
- All dedicated firewalls used in production must follow the University firewall management standard which includes the ability to review currently configured firewalls rules across the organization, identify shadow or redundant rules and rules in conflict, and standardization of device names
- Firewall Rulesets and Configurations must be backed up frequently to alternate storage (not on the same device). Multiple generations must be captured and retained in order to preserve the

integrity of the data, should restoration be required. Access to rulesets and configurations and backup media must be restricted to those responsible for administration and review.

Firewall Rules

Firewall rules specify (either allow or deny) the flow of traffic through the firewall device. Firewall rules are typically written based on a source object (IP address/range, DNS Name, or group), destination object (IP address/range, DNS Name, or group), Port/Protocol and action.

- All Firewall implementations should adopt the principal of "least privilege" and deny all inbound traffic by default. The Ruleset should be opened incrementally to only allow permissible traffic.
- Outbound traffic should be enumerated for data stores, applications, or services
- Overtly broad rules may be allowed for specific groups of individuals (not systems)
- The use of overly permissive firewall rules is prohibited (i.e. ANY/ANY/ALL rules)
- Protocols defined in services and in the firewall must utilize Service Name and Protocol/Port information as assigned by IANA unless there is a technical reason to do otherwise other than "security through obscurity"

Firewall Logging

Firewall log integrity is paramount to understanding potential threats to the network. Firewall devices must log the following data to a system outside of the physical firewall itself and must be regularly reviewed. Firewall logs may be forwarded to the ISO SIEM for retention and analysis.

The following items must be logged as part of the operation of the firewall:

- All changes to firewall configuration parameters, enabled services, and permitted connectivity
- Any suspicious activity that might be an indicator or either unauthorized usage or an attempt to compromise security measures

ENFORCEMENT

Violations of this policy may result in appropriate disciplinary measures in accordance with University By-Laws, General Rules of Conduct for All University Employees, applicable collective bargaining agreements, and the Student Code.

Questions about this policy or suspected violations may be reported to any of the following:

Office of University Compliance - https://compliance.uconn.edu (860-486-2530)
Information Technology Services Tech Support - https://techsupport.uconn.edu (860-486-4357)
Information Security Office – https://security.uconn.edu

POLICY HISTORY

Policy created: September 24, 2020
Revisions: