NIST 800-171 Security Standard

The National Institute of Standards and Technology (NIST) publishes the 800-171 security requirements, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations. The purpose of that publication is to provide guidance for government contractors to protect certain types of federal information. NIST 800-171 is a subset of security controls derived from the NIST 800-53 publication. This subset of security controls is required when a non-federal entity is sharing, collecting, processing, storing or transmitting "Controlled Unclassified Information (CUI)" on behalf of a federal government agency.

Compliance with this standard, plus all Office of Information Security Policies, Standards and Procedures is required to achieve NIST compliance.

NIST 800-171 Control Number	NIST 800-171 Security Standard
Access Control	
3.1.1	Access to systems storing or processing CUI should be limited to authorized users or authorized processes acting on behalf of authorized users. Authorized users and processes should be identified. System access should be granted using university enterprise identity management tools such as active directory and/or university approved privileged access management solution.
3.1.2	Users are only permitted to engage in transactions and function for which they are authorized, and which are defined.
3.1.3	Any system that contains CUI should provide documentation of the data flow. This documentation should include firewalls, proxies, encryption, and other security technologies. Identify source and destination for CUI and who is authorized to control the flow of the data.
3.1.5	Employ the principle of least privilege. Users should only be granted enough system privileges to allow them to fulfill their job duties. Security functions are identified.

3.1.7	On any system with CUI only privileged users should be able to complete privileged functions and those functions should be captured in audit logs. Non-privileged users should also be defined, and they should be prevented from executing privileged functions.
3.1.9	Logon screen should display appropriate notices for any system with CUI. Privacy and security notices should be displayed.
3.1.11	Conditions requiring a user session to be terminated should be defined and automatically terminate after the defined conditions occur.
3.1.12	Remote access to systems with CUI should be identified, monitored, and controlled.
3.1.13	Remote access session should use an approved encryption method while the data is in transit.
3.1.14	Remote access must use a university approved method, currently Cisco AnyConnect VPN is the approved method.
3.1.15	Remote access for privileged actions and commands are identified. Access to security-relevant information is identified and authorized.
3.1.17	Wireless access must use authentication and encryption.
3.1.18	Mobile devices that process, store or transmit CUI are identified. Mobile devices should be authorized. Connections from mobile devices should be monitored and logged using university approved tools such as the enterprise installation of Splunk.
3.1.19	Mobile devices that process, store or transmit CUI must be encrypted.
3.1.20	Guidelines and restrictions will be placed on the use of personally owned or external system access. Only authorized individuals will be permitted external access and those systems must meet the security standards set out by the organization.
3.1.21	Portable storage devices containing CUI should be documented and encrypted.
3.1.22	Only university authorized individuals may post information on publicly accessible systems. Public information should be reviewed annually to ensure that non-public information is not posted. The individuals authorized to post information on publicly accessible sites should be identified and procedures should be in place to ensure CUI is not posted publicly. Procedures should be in place to review publicly available information before and after it is posted. Procedures should include a method for removing improper posting of CUI.
Awareness and Training	
3.2.1	Users, managers, and system administrators should receive initial and annual security training titled “IT@UC Information Security Annual Training”.
3.2.2	Users of CUI must be adequately training to carry out their assigned information security-related duties.
3.2.3	Security awareness training should Include potential indicators associated with insider threats.
Audit and Accountability	
3.3.1	System that process, store or transmit CUI must forward audit logs the IT@UC enterprise Splunk environment. Audit logs need to enable the monitoring, analysis, investigation and reporting of unlawful or unauthorized system activity.
3.3.3	The organization reviews, defines and updates audited events annually or in the event of substantial system changes.
3.3.4	The information system alerts personnel with security responsibilities in the event of an audit processing failure and maintains audit records on host servers until log delivery to central repositories can be re-established.
3.3.5	Splunk will be used to correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.
3.3.6	Systems that process, store or transmit CUI must forward audit logs the IT@UC enterprise Splunk environment. Splunk supports report capabilities.
3.3.7	Information systems should use a university approved authoritative source to compare and synchronize internal clocks, such as ntp.uc.edu.

Configuration Management	
3.4.1	Systems that store or process CUI should utilize an established and maintained baseline for that include hardware, software, firmware and documentation. A systems inventory shall be maintained that includes hardware, software, firmware and documentation.
3.4.2	Establish and enforce security configuration settings for information technology products employed in organizational information systems.
3.4.3	System changes will be tracked, reviewed, approved or disapproved, and documented. Change control tracking will be audited annually.
3.4.4	Appropriate university personnel will conduct a security impact analysis prior to change implementation.
3.4.5	Hardware, software or firmware changes must be performed by qualified and authorized individuals. These access restrictions should be defined, documented and approved.
3.4.6	Employ the principle of least functionality by configuring the information system to provide only essential capabilities.
3.4.7	Systems that store or process CUI should Restrict, disable and prevent the use of nonessential programs, functions, ports, protocols and services. Essential programs, functions, ports, protocols and services are defined. Non-essential programs, functions, ports, protocols and services are defined, disabled or restricted.
3.4.8	Apply deny-by-exception policy to prevent the use of unauthorized software or deny-all, permit-by-exception policy to allow the execution of authorized software.
Identification and Authentication	
3.5.3	Access to privileged accounts that store or process CUI must use multifactor authentication.
3.5.4	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.
3.5.5	University accounts will be assigned and managed by the university's central identity management system. Accounts are provisioned as part of the established account creation process. Accounts are uniquely assigned to faculty, staff, students and affiliates. Usernames are not reused.
3.5.6	User accounts or identifiers associated with a project or contract covered by NIST 800-171 are monitored for inactivity. Account access to the in-scope systems after 180 days of inactivity.
3.5.11	Obscure feedback, such as error message, of authentication information.
Maintenance	
3.7.2	Tools, techniques, mechanisms and personnel used to conduct system maintenance on systems that contain CUI must by controlled and documented.
3.7.4	Media used by maintenance personnel for troubleshooting, diagnostics or other maintenance must be scanned with anti-virus software such as McAfee prior to use.
3.7.5	Remote access for maintenance or diagnostics must occur via an approved remote solution using multi-factor authentication. A remote session must be disconnected when maintenance is complete.
Media Protection	
3.8.1	Protect system media containing CUI, paper and digital. Controlling system media includes conducting inventories, maintaining accountability, and ensuring procedures are in place to allow individuals to check out and return stored media.
3.8.2	Limit access to systems that process or store CUI to only authorized users.
3.8.4	Media containing CUI should be marked with the necessary sensitive data markings and distribution limitations. See the CUI Marking Handbook for information.
3.8.5	Control access to media containing sensitive data and maintain accountability for media during transport outside of controlled areas.

3.8.7	Control the use of removable media on information system components. Removable media must be encrypted with a university approved encryption system such as McAfee File and Removable Media Protection software.
3.8.8	Only documented portable storage devices with an identifiable owner are to be used to store CUI data.
3.8.9	Data backup media should be encrypted to protect confidentiality of information at designated storage locations.
Physical Protection	
3.10.2	Protect and monitor the physical facility and support infrastructure for university systems. This can be accomplished by guards, sensor devices or video surveillance.
3.10.5	Physical access devices (such as card readers, proximity readers, and locks) will be maintained and operated according to the manufacturer recommendations. These devices will be updated with any changed access control information as necessary to prevent unauthorized access. The university will review the location and type of each physical access device and evaluate its suitability for the organization's needs.
Risk Assessment	
3.11.1	Data Stewarts will provide an initial and periodic risk assessment. Changes in the environment that may affect the system or service, changes in use of or infrastructure will be documented and assessed as modified. The impact analysis is to be a living document and incorporated into a larger risk assessment profile for the system/service.
Security Assessment	
3.12.1	An annual security assessment will be conducted to ensure that security controls are implemented correctly and meet the security requirements for the compliance environment. The assessment scope includes all information systems and networks in or directly connected to the compliance environment and all security controls and procedures necessary to meet the compliance requirements of the environment. The assessment will include, but is not limited to, vulnerability scanning, penetration testing, security control testing and reviews, configuration testing and reviews, log reviews, and personnel interviews. A representative sampling of systems will be assessed. Information Security, or an independent security auditor, will conduct the assessment.
3.12.3	Continuous monitoring tools will be deployed for front Internet facing systems or those used to store or transmit sensitive data. At a minimum, systems will be monitored for privileged access, permission changes, kernel modifications, and binary changes, against a control and system baseline. Continuous monitoring reports and alerts will be reviewed daily. Unauthorized changes or unauthorized access will be reported to the Office of Information Security within 24 hours of it being reported.
3.12.4	Develop, document, and periodically update systems security plans (SSP) that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationship with or connections to other systems. The update frequency to the systems security plans need to defined and updated within the specified timeframe.
System and Communication Protection	
3.13.1	Monitor, control and protect organizational communications at the external boundaries and key internal boundaries of the information systems. This includes gateways, routers, firewalls, VPNs, organizational DMZs that are used to protect CUI. Restrict external web traffic to only designated servers.
3.13.2	Employ architectural designs, software development techniques and systems engineering principles that promote effective information security within organizational information systems.
3.13.3	Separate user functionality from information system management functionality. System user functionality and system management functionality is identified. System user functionality is separated from system management functionality.
3.13.4	Prevent unauthorized and unintended information transfer via shared system resources.

3.13.5	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
3.13.6	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). Document all exceptions to the “deny all” policies.
3.13.7	University approved VPN must be used for remote devices. Devices the store, process or access CUI should not use split tunneling in remote devices.
3.13.8	CUI data must be encrypted during transmission unless otherwise protected by alternative physical safeguards.
3.13.9	Outline the controls for terminating network connections at the end of the sessions or after a defined period of inactivity for both internal and external networks.
3.13.10	Cryptography keys for devices are management in McAfee ePolicy Orchestrator using McAfee Management of Native Encryption product.
3.13.11	Use FIPS-validated cryptography to protect the confidentiality of sensitive data.
3.13.12	Disable the ability for remote activation of collaborative computing devices from systems housing CUI (e.g. cameras, microphones, etc.) and notify users when collaborative computing devices are in use.
3.13.13	Control and monitor the use of mobile code. Define limits of mobile code usage, establish usage restrictions and specifically authorize use of mobile code (e.g. Java, ActiveX, Flash, etc.) within systems that store or process CUI.
3.13.14	Define and establish usage restrictions and specifically authorized the necessary use of VoIP technologies within information systems.
3.13.15	Outline the controls implemented to protect session communications (e.g., the controls implemented to validate identities and information transmitted to protect against MITM attacks, session hijacking, and insertion of false information into sessions).
3.13.16	Outline the controls used to protect the confidentiality of sensitive data at rest while stored in a university system.
System and Information Integrity	
3.14.2	The university will employ malicious code protection mechanisms at information system entry and exit points to minimize the presence of malicious code. These protection mechanisms may include firewalls, electronic mail servers, webservers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices.
3.14.3	The university will receive security alerts, advisories, and directives from reputable external agencies, and disseminate this information to individuals with need-to-know in the organization. In the event of alerts, advisories, or directives that have widespread impact on the organization, internal security directives will be disseminated directly to information system users, managers, and administrators.
3.14.4	Update malicious code protection mechanisms in a timely manor.
3.14.5	Systems that store or process CUI must have the Qualys agent installed, and university approved anti-virus software such as McAfee installed. Systems will be scanned monthly. Anti-virus software must be configured to enable real-time scanning of files from external sources.
3.14.6	The university will monitor the information system to detect attacks and indicators of potential attacks, as well as unauthorized local, network, and remote connections. The university will use logs collected in Splunk and other security tools to collect essential information system. Information gained from these monitoring tools will be protected from unauthorized access, modification, and deletion.
3.14.7	The university will monitor systems to identify unauthorized access and use, as well as potential misuse of the information system. Authorized use of a system should be defined. Unauthorized use of the system is identified.

Related Links

NIST 800-171 rev-2
Office of Information Security Policies, Procedures and Standards
CUI Marking Handbook

Contact Information

IT@UC Office of Information Security 513-558-ISEC (4732) Email: infosec@uc.edu