UNT System NIST 800-171 Rev 2 Standards

UNT System™

Information Technology

Version 1.0

Published 10/22/2025

INTRODUCTION

UNT System must protect Controlled Unclassified Information (CUI) in accordance with UNT System Regulation 04.10000 Controlled Unclassified Information Protection and the regulations, policies, and standards that make up the UNT System CUI Protection Program.

This standard identifies the controls required for CUI protection when the Cybersecurity Maturity Model Certification and NIST 800-171 Rev. 2 are in scope, including but not limited to CUI for research projects sponsored by the U.S. Department of Defense or other federal agency.

CONTROL REQUIREMENTS

1. ACCESS CONTROL

a. Controlled Environment access must be limited to authorized users only. Access must be authorized to the types of transactions and functions that authorized users are permitted to execute. System Administrators must follow the UNT System Information Security Handbook and Access Control Standard to ensure that users are only granted access based on access authorizations and the Principle of Least Privilege. User functionality must be limited to basic system functions and administrative and security functions limited to System Administrators and the institutional Information Security Officers.

b. The flow of CUI in the systems subject to NIST 800-171 requirements must be controlled in accordance with approved access authorizations. CUI may only reside in Controlled Environments.

c. Separation of duties must be established for Controlled Environments that support and contain Controlled Unclassified Information. Separation of duties ensures the reduction of risk to the Controlled Environment.

d. Access authorizations for Controlled Environments must specify the type of access a user needs. System Administrators will only grant access to Users of Controlled Environments based on the Principle of Least Privilege, including for specific security functions and privileged accounts.

e. Users of Controlled Environments must use non-privileged accounts or roles when accessing nonsecurity functions. Security functions must only be performed through the use privileged accounts. Privileged access accounts are limited to System Administrators and institutional Information Security Officers.

f. Users are prohibited from executing privileged functions and all privileged functions executed by System Administrators and Information Security Officers must be captured in audit logs.

g. System Administrators must configure Controlled Environments to lockout users after 5 unsuccessful logon attempts for a period of 15 minutes or more in accordance with the UNT System Information Security Handbook section PR.18.

h. System Administrators of Controlled Environments must configure systems to display the following privacy and security notice prior to any user accessing a Controlled Environment:

    a. This system is the property of the University of North Texas System and your use of this resource constitutes an agreement to abide by relevant federal and state laws and institutional policies. Unauthorized use of this system is prohibited. Violations can result in penalties and criminal prosecution. Usage may be subject to security testing and monitoring. Users have no expectation of privacy except as otherwise provided by applicable privacy laws. This information system contains CUI with specific requirements imposed by the Department of Defense and use of this information system may be subject to other specified requirements as associated with certain types of CUI such as Export Controlled Information. Continued use of this system indicates consent to these terms and conditions.

i. Information System/Application Owners must establish session locks with pattern-hiding displays for all Controlled Environments to prevent access and viewing of data after a period of inactivity. Users must initiate a device lock before leaving a system unattended.

j. System Administrators must configure Controlled Environments to automatically terminate a user session after 12 hours of inactivity, with the exception of long running programmatical sessions.

k. System Administrators must monitor and control remote access sessions in accordance with the UNT System Information Security Handbook section PR.19.

l. System Administrators must employ cryptographic mechanisms to protect the confidentiality of remote access sessions in accordance with the UNT System Information Security Handbook section PR.4 and the Cryptographic Controls Standard.

m. System Administrators must only route remote access through authorized and managed access control points.

n. System Administrators must authorize remote execution of privileged commands and remote access to security-relevant information in a format that provides evidence and as documented in the System Security Plan for the Controlled Environment.

o. System Administrators must authorize devices allowed for wireless access prior to allowing such connections.

p. System Administrators must protect wireless access using Enterprise authentication and encryption in accordance with the UNT System Information Security Handbook section PR.4 and the Cryptographic Controls Standard.

q. Users are prohibited from utilizing personal mobile devices to connect to Controlled Environments. Users may only access Controlled Environments through UNT System hardware assets. UNT System hardware assets must be up to date with all patches and vulnerabilities remediated prior to accessing Controlled Environments.

r. Users must encrypt all CUI created or maintained on UNT System managed mobile device assets. System Administrators must ensure that Controlled Environments encrypt CUI in transit and at rest in accordance with the UNT System Information Security Handbook section PR.4 and the Cryptographic Controls Standard.

s. The UNT System Chief Information Security Officer or their designee must verify and control the connection to Controlled Environments and use of external systems when creating, processing, or storing CUI. External systems must be FedRAMP Moderate or High authorized prior to consideration for connection or use. UNT System Cybersecurity and IT Compliance must update System Security Plans and system diagrams to reflect connection and use of external systems to ensure compliance with relevant statutory and contractual requirements.

t. Users must limit the use of portable storage devices on external systems within Controlled Environments according to the UNT System Information Security Handbook PR.8.

u. Users and System Administrators are prohibited from posting or processing CUI on publicly accessible systems, including but not limited to, websites and systems with ports openly available to the internet.

2. AWARENESS AND TRAINING

a. System administrator, managers, and users of Controlled Environments must complete training to ensure they are capable of carrying out their assigned duties

and responsibilities with awareness for the security risks associated with their activities.

b. System Administrators, managers, and Users of Controlled Environments must acknowledge their responsibilities to comply with applicable policies, standards, and procedures related to the security of those Controlled Environments.

c. System Administrators and Users of Controlled Environments must complete security awareness training on recognizing and reporting potential indicators of insider threat.

3. AUDIT AND ACCOUNTABILITY

a. System audit logs of Controlled Environments must be created and retained to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. System audit logs for Controlled Environments must be retained for a minimum of one year.

b. System Administrators must ensure that the actions of users can be uniquely traced to those users, so they can be held accountable for their actions, in accordance with the UNT System Information Security Handbook section DE.4 and Logging Management Standard.

c. System Administrators must review and update logged events in accordance with the UNT System Information Security Handbook section DE.4 and the Logging Management Standard.

d. Controlled Environments must be configured to alert System Administrators in the event of an audit logging process failure. System Administrators must take action to resolve audit logging process failures immediately.

e. System Administrators must configure Controlled Environments to correlate audit record review, analysis, and reporting to ensure the success of investigations and responses to indications of unlawful, unauthorized, suspicious, or unusual activity.

f. System Administrators should provide audit record reduction and report generation to support on- demand analysis and reporting in accordance with the Logging Management Standard.

g. System Administrators must configure Controlled Environments to compare and synchronize internal system clocks with an authoritative source to generate time stamps for audit records.

h. System Administrators must protect audit information and audit logging tools from unauthorized access, modification, and deletion.

i. Management of audit logging functionality is limited to System Administrators.

4. CONFIGURATION MANAGEMENT

a. System Administrators must establish and maintain baseline configurations of Controlled Environments in accordance with the UNT System Information Security Handbook section PR.5 and the Secure Configuration Management Standard.

b. System Administrators must establish and maintain inventories of organizational systems in Controlled Environments (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

c. System Administrators must establish and enforce security configuration settings for information technology products employed in Controlled Environments.

d. System Administrators must track, review, approve or disapprove, and log changes to organizational systems in accordance with the UNT System Information Security Handbook section PR.6 and the Change Enablement Standard. The Change Advisory Board must analyze the security impact of changes prior to implementation.

e. Only System Administrators may initiate and implement changes to Controlled Environments, ensuring that physical and logical access restrictions associated with changes to Controlled Environments are defined, documented, and approved.

f. System Administrators must employ the principle of least functionality by configuring organizational systems and assets in Controlled Environments to provide only essential capabilities.

g. System Administrators must restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services in Controlled Environments.

h. System Administrators must apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by- exception (whitelisting) policy to allow the execution of authorized software.

i. System Administrators must control and monitor installed software in Controlled Environments.

j. Users are prohibited from installing unauthorized software in Controlled Environments.

5. IDENTIFICATION AND AUTHENTICATION

a. Information Resource/Application Owners and System Administrators must establish controls and measures that uniquely identify and authenticate Users to ensure all actions within the Controlled Environment are traceable and attributed to the User.

b. System Administrators must ensure that identities are authenticated for Users, automated processes, or devices, as a prerequisite to allowing access to Controlled Environments.

c. Users must authenticate to Controlled Environments through multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts**.**

d. System Administrators must employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.

e. System Administrators must implement password requirements for Controlled Environments that meet or exceed password standards established in the UNT System Information Security Handbook section PR.18, including but not limited to complexity and cryptography.

f. System Administrators using temporary passwords for system logons must immediately change to a permanent password.

g. System Administrators must ensure authentication feedback for Controlled Environments is obscured during user authentication.

6. INCIDENT RESPONSE

a. Users and System Administrators must immediately report security and privacy incidents for Controlled Environments to the UNT System Chief Information Security Officer or their designee in accordance with the UNT System Information Security Handbook section RS.1.

b. The UNT Chief Information Security Officer and their designees will track, document, investigate, report, and respond to security and privacy incidents in accordance with the UNT System Incident Response Plan and supporting Standard Operating Procedures.

c. The UNT System Chief Information Security Officer and their designees must annually test the organizational incident response capability.

7. MAINTENANCE

a. System Administrators are responsible for performing maintenance on organizational systems within Controlled Environments, including patching and updating resources.

b. System Administrators must implement controls in accordance with the UNT System Information Security Handbook for all tools, techniques, mechanisms, and personnel used to conduct system maintenance.

c. System Administrators and Users must ensure that equipment in Controlled Environments is sanitized of any CUI if removed for off-site maintenance.

d. System Administrators must ensure that media containing diagnostic and test programs are verified for malicious code prior to being used in Controlled Environments. If, upon inspection of media containing maintenance, diagnostic, and test programs, the System Administrator determines that the media contains malicious code, the System Administrator will immediately report this discovery as an incident to the UNT System Chief Information Security Officer or their designee to ensure the incident is handled consistent with the UNT System Incident Response Plan and supporting Standard Operating Procedures.

e. Multifactor authentication is required for all nonlocal maintenance sessions occurring via external network connections and System Administrators must terminate session connections when nonlocal maintenance is complete.

f. Information System/Application Owners must supervise the on-premises maintenance activities of maintenance personnel without required access authorization.

8. MEDIA PROTECTION

a. Users must physically control and securely store any system media containing CUI, both paper and digital.

b. Only authorized users may access CUI on system media. Authorized Users are those identified by Information Owners or campus Research Security Officers through Technology Control Plans, as applicable.

c. Users and System Administrators must sanitize or destroy system media containing CUI before disposal or release for reuse.

d. Users and System Administrators must mark media with necessary CUI markings and limit its distribution to those authorized by the Information Owner and campus Research Security Officer as outlined in the Technology Control Plan, as applicable.

e. Users and System Administrators must control access to media containing CUI and maintain accountability for media during transport outside of Controlled Environments.

f. Users and System Administrators must ensure that all media containing CUI be protected through encryption in accordance with the UNT System Information Security Handbook section PR.4 and PR.8 and the Cryptographic Controls Standard.

g. Users and System Administrators must control the use of removable media on system components in Controlled Environments.

h. The use of portable storage devices in Controlled Environments is strictly prohibited unless such devices have an identified owner authorized by the Information Owner and campus Research Security Officers, as applicable.

i. System Administrators must protect the confidentiality of backup CUI at storage locations and ensure backups comply with the UNT System Information Security Handbook section PR.7.

9. PERSONNEL SECURITY

a. Users of Controlled Environments must be screened prior to being authorized access to systems containing CUI, in accordance with UNT System Regulation 06.10000 Controlled Unclassified Information Protection.

b. System Administrators must ensure that systems in Controlled Environments containing CUI are protected during and after personnel actions such as terminations and transfers by disabling access immediately upon notice and conducting annual user reviews and quarterly privileged access user reviews.

10. PHYSICAL PROTECTION

a. System Administrators must limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.

b. System Administrators must protect and monitor the physical facility and support infrastructure for Controlled Environments.

c. System Administrators must escort visitors and monitor visitor activity in Controlled Environments.

d. System Administrators must maintain audit logs of physical access to Controlled Environments.

e. System Administrators must control and manage physical access devices within Controlled Environments.

f. Users must meet or exceed all controls of the UNT System Information Security Handbook and this standard when accessing CUI at alternate work sites.

11. RISK ASSESSMENT

a. UNT System Cybersecurity and IT Compliance and campus Research Security Officers, as applicable, will annually assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of Controlled Environments and the associated processing, storage, or transmission of CUI.

b. System Administrators must regularly scan for vulnerabilities in Controlled Environments and when new vulnerabilities affecting those systems and applications are identified. Vulnerabilities must be remediated in accordance with the UNT System Information Security Handbook section DE.1 and the Vulnerability Management Standard.

c. System Administrators must remediate vulnerabilities in accordance with those discovered in risk assessments and in accordance with the UNT System Information Security Handbook section DE.1 and the Vulnerability Management Standard.

12. SECURITY ASSESSMENT

a. UNT System Cybersecurity and IT Compliance will annually assess the security controls of Controlled Environments to determine if the controls are effective in their application.

b. UNT System Cybersecurity and IT Compliance must develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. Plans of action must be remediated within 180 days of identification.

c. UNT System Cybersecurity and IT Compliance must monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

d. UNT System Cybersecurity and IT Compliance must develop, document, and annually update System Security Plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

13. SYSTEM AND COMMUNICATIONS PROTECTION

a. System Administrators must monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.

b. System Administrators must employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within Controlled Environments.

c. System Administrators must assign User access to perform limited functionality, separate from system management functionality. Only System Administrators may have access to manage system functionality.

d. The transfer of information must be strictly controlled and reside only in Controlled Environments. System Administrators must prevent unauthorized and unintended information transfer via shared system resources.

e. System Administrators must implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

f. System Administrators must configure Controlled Environments to deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

g. System Administrators must prevent remote devices from simultaneously establishing non-remote connections with Controlled Environments through split tunneling.

h. Users and System Administrators must encrypt CUI in transmission to prevent unauthorized disclosure in accordance with the UNT System Information Security Handbook section PR.4 and Cryptographic Controls Standard.

i. System Administrators must configure Controlled Environments to terminate internal and external network connections associated with communications sessions at the end of the sessions or after 8 hours of inactivity, with the exception of long-running programmatical sessions.

j. System Administrators must establish and manage cryptographic keys for cryptography employed in Controlled Environments in accordance with the UNT System Information Security Handbook section PR.4 and the Cryptographic Controls Standard.

k. System Administrators must employ FIPS-validated cryptography when used to protect the confidentiality of CUI in accordance with the Cryptographic Controls Standard.

l. Users and System Administrators are prohibited from utilizing remote activation collaborative computing devices within Controlled Environments.

m. System Administrators must control and monitor the use of mobile code. Mobile code includes any program, application, or content that can be transmitted across a network (e.g., embedded in an email, document, or website) and executed on a remote system.

n. System Administrators must control and monitor the use of Voice over Internet Protocol (VoIP) technologies in Controlled Environments.

o. System Administrators must protect the authenticity of communications sessions at the sessions level, not the packet level.

p. System Administrators must establish cryptography at rest for CUI.

14. SYSTEM AND INFORMATION INTEGRITY

a. System Administrators must Identify, report, and correct system flaws in accordance with the UNT System Information Security Handbook and the Vulnerability Management Standard.

b. System Administrators must provide protection from malicious code at designated locations within Controlled Environments, including but not limited to, complying with the UNT System Mandate SEC.0001 Crowdstrike Endpoint Security Solution Compliance.

c. The UNT System Chief Information Security Officer or their designee must monitor system security alerts and advisories and take action in response.

d. System Administrators must update malicious code protection mechanisms when new releases are available.

e. System Administrators must perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.

f. System Administrators must monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

g. System Administrators must Identify unauthorized use of organizational systems in Controlled Environments.

APPENDIX A - GLOSSARY

1. Controlled Environment. "Controlled Environment" means any physical area or space and Technology Environment with adequate physical, technical, administrative, and procedural controls, preventing the unauthorized access or disclosure of Controlled Unclassified Information (CUI).

2. Controlled Unclassified Information (CUI). "Controlled Unclassified Information" means information the U.S. government creates or possesses; or that an entity creates or possesses for or on behalf of the U.S. government; that a law, regulation, or U.S. government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. CUI does not include information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and U.S. government-wide policies that is classified under Executive Order 13526 or the Atomic Energy Act, as amended.

3. Cybersecurity Maturity Model Certification. "Cybersecurity Maturity Model Certification" means the program established by the U.S. Department of Defense (DoD) to standardize security practices and processes intended to protect Federal Contract Information (FCI) and CUI.

4. Information Owner. "Information Owner" means the individual with operational authority for specific information and who is responsible for authorizing the controls for the generation, collection, processing, access, dissemination, and disposal of that information.

5. Information System/Application Owner. "Information System/Application Owner" means Custodians who are responsible for the development, procurement, integration, modification, operation and maintenance, implementation of the Information Owner-defined controls, and/or final disposition of an information resource.

6. Principle of Least Privilege. The security principle that requires the application of the most restrictive privileges needed for performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

7. System Administrator. "System Administrator" means the custodians responsible for the installation and maintenance of an information resource, providing effective information resource utilization, adequate security parameters, and sound implementation of established policy and procedures

8. System Security Plan (SSP). "System Security Plan" means a formal document that outlines the security requirements and controls for a computer or information system. The SSP identifies system components, describes the environment, and explains how security requirements are implemented.

9. Technology Control Plan. “Technology Control Plan” means a customized data management document that outlines the appropriate access and handling procedures to protect certain types of Controlled Unclassified Information (CUI), including but not limited to: Export-Controlled Information and Controlled Technical Information.

10. Technology Environment. “Technology Environment” means the computing and storage systems including, but not limited to, hardware, software, servers, datacenter, and cloud storage where CUI is processed and stored and the physical infrastructure that houses these systems.

11. User. “User” means an individual or automated application authorized to access an information resource in accordance with the Information Owner-defined controls and access rules. UNT System Users include, but are not limited to, faculty, staff, guests, and contractors.

APPENDIX A – VERSION LOG

Date	Approved By	Version	Notes
10/27/2025	Rich Anderson	1.0	New NIST 800-171 Rev 2 Standard