PI's NIST SP 800-171 Security Control Requirements

UConn Secured Research Infrastructure (SRI)
Information System Owner (Principal Investigator) Checklist Summary

UConn, as a nonfederal institution that is to follow the NIST SP 800-171 security control requirements as required due to the DFARS 252.204-7012 clause and Export Control (ITAR/EAR) as notified by the OVPR, the Information System Owner/Principal Investigator (PI) is a University official responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system and agrees with the following checklist.

☑ The research project's identified CUI data is to be maintained in the SRI environment's approved locations that adhere to the NIST 800-171 security controls.

- On the secured S: data storage drive that all researches will have shared access
  - The SRI virtual workstation desktop is not encrypted.
- On an approved and designated SRI laptop that was reimaged and configured by ITS
  - The SRI laptop can store CUI data on its local hard drive and will have access to the research group shared S: drive.
- On an ITS approved NIST SP 800-171 system.
- On an encrypted USB thumb drive.
- Any exceptions will need the proper approval through ITS-ISO and their government sponsor.

☑ Any changes to the research personnel should be notified to their local System Admin and ITS-ISO.

- CUI and information systems containing CUI are to be protected during and after personnel actions such as terminations and transfers.
- Alert the CISO and ITS-ISO on unauthorized use.

☑ Protect, physically control, and securely store information system media containing CUI, both paper and in digital formats.

- All those working with CUI in the SRI will be aware of their surroundings to help prevent unauthorized disclosure of such information.
- Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.
  - Cryptographic mechanisms are implemented to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative safeguards.

☑ PI, local Systems Admin, government sponsors, and external vendors collaborate to ensure only secure (encrypted) protocols are utilized for any CUI data transfer. The PI is responsible for safeguarding system media.

- All CUI data under the DFARS clause must be encrypted and kept in a secure environment. All CUI data on media will be encrypted or physically locked prior to transport outside of the institutions secure locations.
- If a USB must be used, it must be an encrypted USB drive (e.g. BitLocker for Windows).
- All CUI data outside of the SRI environment (e.g. thumb drives, printouts, CD/DVDs) are to be kept in locked storage.

☑ Mark media with necessary CUI markings and distribution limitations.

- All CUI systems will be identified with the appropriate label.
  - Any physical client workstation or device containing CUI must be marked CUI. PI and System Admin affixes the provided labels as appropriate.

PI’s NIST SP 800-171 Security Control Requirements

☑ I understand that the SRI network denies network communications traffic by default and allows network communications traffic by exception.

- The PI or System Admin will work with ITS to ensure all information systems are in dedicated networks with appropriate technical controls.
- The PI is to inform ITS, CISO, or ITS-ISO what the current or upcoming the research project needs are (e.g. if Internet access if required in the SRI environment).

☑ Changes or deviations to information system security control configurations that affect compliance requirements will be reviewed and approved by ITS-ISO.

- The PI can authorize software to be installed. If admin rights are needed, the System Admin or Automated Process can install the software or modify applications.
- PI or System Admin responsible for change monitoring and its security impact.

☑ Sanitize or destroy information system media containing CUI before disposal or release for reuse.

☑ Limit access to CUI on information system media to authorized users.

- All activities of maintenance personnel who do not normally have access to a system are monitored.
- Only authorized individuals will post non-CUI information on publically accessible information systems.
- Grant only enough privileges to a system user to allow them to sufficiently fulfill their job duties.

☑ The Office of the Vice President for Research (OVPR) screen prospective users.

- HR, PI, and departmental administrative support screening prospective users as necessary.

☑ Limit physical access to university information systems, equipment, and the respective operating environments to authorized individuals.

- Output devices such as printers are to be placed in areas where their use does not expose data to unauthorized individuals.
- PI responsible for implementing appropriate physical controls and providing control documentation.
- When approved by ITS-ISO, if CUI data or equipment is stored in a non-SRI environment, the PI will designate building area or room as "sensitive" and design physical security protections (including guards, locks, cameras, card readers, etc.) as necessary to limit physical access to the area to only authorized individuals.

☑ The systems will be periodically scanned for common and new vulnerabilities.

- PI is responsible for communicating any changes to information systems to ensure scans are run on all relevant infrastructure.

☑ Mobile and collaborative computing devices are prohibited from connecting directly to CUI network.

☑ PI and System Admin will work with ITS to ensure all information systems are in dedicated networks with appropriate technical controls including protecting the authenticity of communications sessions.

The Principal Investigator is responsible for the above in each research project that contains or may contain CUI as subject to the DFARS clause and Export Control (ITAR/EAR) following the security controls as listed under NIST SP 800-171. The PI, their researchers, and local IT support (designated technical representative or systems administrator) are to have completed the required NIST SP 800-171 training including information security insider threat awareness and understands their role and responsibilities.

UConn NIST SP 800-171 Security Control Requirements

References

NIST Control Number	NIST 800-171 Control Requirements	UConn PI Managed Control Method
Access Control 3.1.1	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	Maintain list of authorized users defining their identity and associated role. Account requests must be authorized before access is granted. • Accounts cannot be shared and must be unique for each authorized user. o e.g. Names and individual UCONN NetIDs • Separation of duties by user or admin account in accordance with the member's job duties and responsibilities. o e.g. UCONN NetIDs and UCONN NetID Admin accounts • Only grant enough privileges to a system user to allow them to sufficiently fulfill their job duties.
Access Control 3.1.2	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	
Access Control 3.1.3	Control the flow of CUI in accordance with approved authorizations.	
Access Control 3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	
Access Control 3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	
Access Control 3.1.18	Control connection of mobile devices.	Mobile devices prohibited from connecting directly to CUI network. • Mobile devices include cell phones or tablets with a SIM card.
Access Control 3.1.19	Encrypt CUI on mobile devices.	
Access Control 3.1.20	Verify and control/limit connections to and use of external information systems.	Restrictions will be placed on the use of personally owned or external system access. External storage devices prohibited except as described in section 3.8 for data protection backup purposes. • Only authorized individuals will be permitted external access. • Encrypted USB thumb drives for data transfer is allowed. • Firewall policies restrict nonessential inbound and outbound network traffic.
Access Control 3.1.21	Limit use of organizational portable storage devices on external information systems.	
Access Control 3.1.22	Control information posted or processed on publicly accessible information systems.	Only authorized individuals will post non-CUI information on publically accessible information systems. • Authorized individuals will be trained to ensure that non-public information is not posted. • Public information will be reviewed annually to ensure that non-public information is not posted.

Awareness and Training 3.2.1	Ensure that managers, systems administrators, and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organizational information systems.	Faculty, staff, and students working in the SRI environment are to receive the NIST SP 800-171 information security training and potential indicators of insider threat. • Personnel with security related responsibilities will receive information security training.
Awareness and Training 3.2.2	Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.	
Awareness and Training 3.2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	
Configuration Management 3.4.3	Track, review, approve/disapprove, and audit changes to information systems.	Changes or deviations to information system security control configurations that affect compliance requirements will be reviewed and approved by ITS-ISO. • PI, IT Designee, or Automated Process only can install software or modify applications. • PI or IT Designee responsible for change monitoring and its security impact.
Configuration Management 3.4.4	Analyze the security impact of changes prior to implementation.	
Configuration Management 3.4.7	Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services.	Permit or deny on an individual basis the installation of authorized software. Only those programs, functions, services, ports and protocols necessary to provide the service of the information system will be configured for that system. • Admin access for users to systems and applications is prohibited (section 3.1). • The PI can authorize software to be installed. If admin rights are needed, the System Admin or Automated Process can install/modify the software/apps. • Systems and/or applications will be accessed by authorized users only, as defined in section 3.1. • Applications and services not necessary to provide the service of the information system will not be configured or enabled. • Control and monitor user-installed software.
Configuration Management 3.4.8	Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	
Configuration Management 3.4.9	Control and monitor user-installed software.	

Identification and Authentication 3.5.2	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	The accounts in use will be assigned and managed by the university's central identity stores (per control 3.5.1). • Accounts are provisioned as part of the established account creation process. Accounts are uniquely assigned to faculty, staff, students upon matriculation, or affiliates when sponsored by an authorized faculty or staff member. • Access to data associated with the project is controlled through role-based authorization by the project's PI.
Maintenance 3.7.1	Perform maintenance on organizational information systems.	Desktops and servers for a DFARS project in the SRI are enrolled in the University Managed Desktop service. • UConn ITS utilizes trained central IT staff and infrastructure supported by central IT (ITS). • Managed Desktop Service has a dedicated and trained staff. • Maintenance will be performed by the IT Designee or ITS.
Maintenance 3.7.2	Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.	
Maintenance 3.7.3	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	Any media that is removed off-site for maintenance or disposal must be sanitized utilizing existing university process for surplus of equipment and destruction of media.
Maintenance 3.7.6	Supervise the maintenance activities of maintenance personnel without required access authorization.	All activities of maintenance personnel who do not normally have access to a system are monitored. • PIs are also responsible for monitoring any maintenance personnel.
Media Protection 3.8.1	Protect (i.e., physically control and securely store) information system media containing CUI, both paper and digital.	Protect (i.e., physically control and securely store) information system media containing CUI, both paper and digital. • Responsible parties for data in these systems will document and ensure proper authorization controls for data in media and print. • PI responsible for safeguarding paper. • All CUI data will be stored in the SRI environment or approved alternative methods.
Media Protection 3.8.2	Limit access to CUI on information system media to authorized users.	Limit access to CUI on information system media to authorized users. • All CUI systems will be managed under least access rules (addressed by 3.1.5).
Media Protection 3.8.3	Sanitize or destroy information system media containing CUI before disposal or release for reuse.	Sanitize or destroy information system media containing CUI before disposal or release for reuse. • All managed data storage will be erased, encrypted or destroyed using mechanisms with sufficient power to ensure that no usable data is retrievable from storage devices identified in the workflow of these systems/services. Also addressed by 3.7.3.

Media Protection 3.8.4	Mark media with necessary CUI markings and distribution limitations.	Mark media with necessary CUI markings and distribution limitations. • All CUI systems will be identified with the appropriate label. • Any physical client workstation or device containing CUI must be marked such. • PI and System Admin affixes the labels as appropriate.
Media Protection 3.8.5	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. • Only approved individuals are to have access to media from CUI systems. • PI responsible for safeguarding system media. • PI must create a log and attestation sheet designed to track external transport of DFARS media.
Media Protection 3.8.6	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	All CUI data under DFARS clause must be encrypted. • All CUI data on media will be encrypted or physically locked prior to transport outside of the institutions secure locations. • If a USB must be used, it must be an encrypted USB drive (e.g. BitLocker for Windows).
Media Protection 3.8.7	Control the use of removable media on information system components.	Removable media is prohibited unless no suitable alternative exists, in which case encrypted removable media must be documented on a per-project basis. The use of portable storage devices are prohibited when there is no identifiable owner. • PI and IT Designee responsible for safeguarding system media and providing control documentation. • Data backups of CUI data will be encrypted on media before removal from a secured location.
Media Protection 3.8.8	Prohibit the use of portable storage devices when such devices have no identifiable owner.	
Media Protection 3.8.9	Protect the confidentiality of backup CUI at storage locations.	
Personnel Security 3.9.1	Screen individuals prior to authorizing access to information systems containing CUI.	Office of the Vice President for Research (OVPR) screen prospective users. • HR, PI, and departmental administrative support screening prospective users as necessary.
Personnel Security 3.9.2	Ensure that CUI and information systems containing CUI are protected during and after personnel actions such as terminations and transfers.	CUI and information systems containing CUI are to be protected during and after personnel actions such as terminations and transfers. • PI responsible for notifying ITS/ISO when a personnel change occurs and PI responsible for disabling or removing any local accounts. • PI and IT Designee must remove user access to systems with CUI immediately following termination or transfer. • ITS disables non-local accounts.

Physical Protection 3.10.1	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	Limit physical access to university information systems, equipment, and the respective operating environments to authorized individuals. • If CUI data or equipment is stored in a non-SRI environment, the PI will designate building area or room as "sensitive" and design physical security protections (including guards, locks, cameras, card readers, etc.) as necessary to limit physical access to the area to only authorized individuals. • Output devices such as printers are to be placed in areas where their use does not expose data to unauthorized individuals. • PI responsible for implementing appropriate physical controls and providing control documentation.
Physical Protection 3.10.3	Escort visitors and monitor visitor activity.	PI responsible for escorting visitors and monitoring activity and providing control documentation when visitors visit the project workspace that contain CUI data. • PI maintains a visitor log and also accompany visitors who are on site.
Physical Protection 3.10.4	Maintain audit logs of physical access.	
Physical Protection 3.10.6	Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites).	All alternate sites where sensitive data is stored or processed must meet the same physical security requirements as the main site. • PI responsible for implementing controls on physical workstation. o Access to CUI on SRI approved systems, ITS data center controls address this requirement.
Risk Assessment 3.11.2	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of CUI.	Systems will be periodically scanned for common and new vulnerabilities. A prioritized action plan to remediate identified weaknesses or deficiencies will be created from the findings reported. • PI is responsible for communicating any changes to information systems to ensure scans are run on all relevant infrastructure. • ITS, ISO, IT Designee, and PI work to address identified vulnerabilities. • ISO responsible for the automation of vulnerability scans.
Risk Assessment 3.11.3	Remediate vulnerabilities in accordance with assessments of risk.	
Security Assessment 3.12.2	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.	

System and Communications Protection 3.13.3	Separate user functionality from information system management functionality.	Ensure system user functionality is separate from system management-related administration (privileged) functionality. • Addressed in Access Control 3.1.
System and Communications Protection 3.13.4	Prevent unauthorized and unintended information transfer via shared system resources.	Prevent unauthorized and unintended information transfer via shared system resources. • PI or System Admin will work with ITS to ensure all information systems are in dedicated networks with appropriate technical controls.
System and Communications Protection 3.13.6	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	Deny network communications traffic by default and allow network communications traffic by exception. • PI or IT designee will work with ITS to ensure all information systems are in dedicated networks with appropriate technical controls.
System and Communications Protection 3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	Cryptographic mechanisms are implemented to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative safeguards. • PI, IT Support Staff/Designee, and External vendors collaborate to ensure only secure (encrypted) protocols are utilized for any CUI data transfer. ○ Data at rest is encrypted on data storage drives. ○ For data in motion, encryption is enabled with a pre-authentication integrity check hash.
System and Communications Protection 3.13.12	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	Collaborative computing devices from information systems housing CUI is denied by default. • If a requirement of PI, prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.
System and Communications Protection 3.13.13	Control and monitor the use of mobile code.	Mobile devices prohibited from connecting directly to CUI network as per Access Control 3.1. • If ever an approved requirement, PI must create required documentation for any software development and use SDLC practices http://sdlc.uconn.edu/sdlc-tools/ including use of mobile code.
System and Communications Protection 3.13.15	Protect the authenticity of communications sessions.	PI and IT Designee will work with ITS to ensure all information systems are in dedicated networks with appropriate technical controls including protecting the authenticity of communications sessions. Derived by control family 3.1 and 3.5.
System and Comm Protection 3.13.16	Protect the confidentiality of CUI at rest.	Protecting the confidentiality of CUI, SRI storage is encrypted (e.g., the S: data storage drive, system TPM encryption enabled, or password encrypting a USB thumb drive).

System and Information Integrity 3.14.4	Update malicious code protection mechanisms when new releases are available.	University centrally maintains myriad systems to monitor and control information systems from malicious code (e.g. antivirus). • Any additional controls must be requested by PI if necessary.
System and Info Integrity 3.14.7	Identify unauthorized use of the information system.	University centrally maintains a SIEM to collect, analyze and alert on unauthorized use as defined by the PI or System Admin.