The University of Texas at El Paso
Policy Guidelines
for
Classified and Controlled Unclassified Information (CCUI)

1. Applicability

1.1 These policy guidelines apply to all UTEP research and sponsored projects and other activities that may acquire, generate, or use *classified* or *controlled unclassified information* (commonly referred to as *sensitive information*). They provide general guidance and direction concerning the handling of such information.

1.2 This document may be supplemented or modified by Vice President of Research letter instructions to Principal Investigators that provide program or project-specific instructions and policy.

1.3 Nothing in this document, or in subsequent Vice President of Research letter instructions, is intended to supersede specific written guidance provided by a sponsoring organization's award notice, contract, task order(s), or other written direction(s), or the overarching requirements of NIST SP 800-171.

2. Overview.

2.1 When a project is intended to involve classified information the sponsoring agency will issue a DD Form 254, Contract Security Classification Specification, which will define access and control measures and provide additional security guidance.

2.2 There are more than 300 laws, regulations and government wide policies that require certain types of information to be safeguarded. Some of the labels or legacy markings used to describe *sensitive but unclassified information* are:

- For Official Use Only (FOUO)
- Controlled Unclassified Information (CUI)
- Sensitive But Unclassified (SBU)
- Limited Official Use (LOU)
- Sensitive Unclassified Information (SUI)
- Law Enforcement Sensitive
- DEA Sensitive
- Official Use Only (OUO)
- DOD Technical Information
- Distribution Statements on Technical Documents
- Sensitive Security Information
- Protected Critical Infrastructure Information

- Unclassified Controlled Nuclear Information
- Export-Controlled Information

2.3 UTEP shall use the term ***controlled unclassified information (CUI)*** rather than *sensitive* information. Controlled Unclassified Information (CUI) is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. To facilitate compliance and assurance of requirements laid out herein, the appendix provides a CUI data checklist.

2.3.1. Because of the wide variety of existing policies and controls it is incumbent on University research programs to obtain an understanding from the funding sponsor(s) concerning:

(a) What kind of information is sensitive?
(b) What are the applicable governing laws, regulations or policies?
(c) What are the exact limits of disclosure?

2.3.2 Any acceptance of and handling of CUI data and projects must be done in compliance NIST SP 800-171, of which all requirements and protections supersede policies herein.

2.3.3 Any acceptance of and handling of CUI data and projects must begin with notification to the assistant facility security officer. The assistant facility security officer will notify the chief information security officer so that the principle investigator my use established UTEP checklists to ensure compliance.

3. Definitions.

3.1 *Access* is the ability and opportunity to obtain knowledge of CUI or classified information.

3.2 *Classified information* is information to which access is restricted by law or regulation to particular individuals or groups. There are various classification levels, including: Top Secret, Secret, and Confidential. In addition to these general classification levels, there are additional constraints on access and dissemination which may be program specific.

3.3 *Cleared person.* A person who has been granted a personnel security clearance by a Cognizant Security Agency of the Executive Branch of the U.S. Government. See *Security Clearance*, below.

3.4 *Controlled Unclassified Information (CUI)* is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended.

3.4.1 For example, consider the DHS description of *sensitive information:* any information, the loss, misuse, disclosure, or unauthorized access to or modification of which could adversely affect the national or homeland security, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. The absence of any sensitivity marking is not a valid basis for assuming that information is non-sensitive.

3.4.2 Such information may be explicitly defined in sponsoring agency documentation, e.g., “information concerning the configuration and dimensions of the wave-form guides in a receiver section is sensitive and will not be disclosed to unauthorized personnel.”

3.4.3 This definition does not necessarily encompass proprietary or trade secret information. Such information is important to the originator but, unless it contains information in the above definition, it is not considered CUI. (Dissemination of proprietary or trade secret information is normally prescribed in non-disclosure agreements or in the award document.)

3.5 *Facility Security Officer/Assistant Facility Security Officer (FSO/AFSO).* The University currently operates its classified information security program under the supervision of the UT System FSO. The University has an AFSO within the Office of Research and Sponsored Projects.

3.6 *Need-to-Know* is the determination by a Principal Investigator or other appropriate University official that a specific person requires access to specific CUI or classified information in order to perform or assist in a lawful and authorized university activity.

3.7 *NISPOM* is the National Industrial Security Program Operating Manual. Promulgated by the Defense Security Service, the NISPOM establishes the standard procedures and requirements for all government contractors, with regards to classified information. Agency specific policies may also apply, especially when dealing with organizations within the Intelligence Community.

3.8 *Safeguarding* means measures and controls that are prescribed to protect CUI or classified information from unauthorized access and to manage the risks associated with processing, storage, handling, transmission, and destruction of such information.

3.9 *Security Clearance* is an administrative determination by competent authority (of the Executive Branch of the U.S. Government) that an individual is eligible, from a security stand-point, for access to classified information of the same or lower category as the level of the clearance granted. Clearances are normally granted by the Defense Security Service, the Department of Energy, the Nuclear Regulatory Commission, or by the CIA/Intelligence Community.

4. Right to Publish.

4.1 While UTEP desires to protect its right to publish the results of University-based research, one should not publically release any information (classified/unclassified) that is tied to a Classified Government Contract without approval from that Contract's Sponsor. External sponsors and the University recognize that researchers may work in areas and develop knowledge that may be controlled unclassified information. In order to allay sponsor and University concerns over the unauthorized release of CUI or classified information, it is University policy that **UTEP personnel will review their manuscript drafts, website postings, brochures, presentations materials (video, slides, posters, etc.), technology transfer information, and all other information that may be disclosed to the public or persons without a need-to-know, to preclude inclusion of CUI or classified information**. This requirement is extended to research sub-award personnel.

5. Safeguarding CUI and Classified Information.

5.1 In the event of conflict, the sponsoring organization's directives take precedence.

5.1.1. Defining the parameters. Principal Investigators are responsible for obtaining the sponsoring organization's guidance concerning:

a. What information is CUI or classified? In the case of the latter, the DD form 254 should provide general classification guidance. For the former, consultation with the sponsoring agency's program officer is advised.
b. What are the applicable governing laws, regulations or policies?
c. What are the exact limits of disclosure?
d. Who can be granted access? For classified information this access is limited to those with proper security clearance and need-to-know. For CUI, consultation with the sponsoring agency's program officer is advisable.

5.1.2. Access.

a. Principal Investigators are responsible to determine who will have access to CUI and/or classified information obtained or generated through their project activities, consistent with the guidance of the sponsoring organization.
b. Access to classified information is limited to appropriately cleared persons with need-to-know.
c. Access to CUI is normally restricted to US citizens with need-to-know, though sponsoring agencies may make exceptions for operational or other reasons.
d. An up-to-date access roster will be maintained. It will be available to all authorized personnel so they may readily identify who is authorized access to any CUI or classified information handled by the project. This roster will include people who are directly involved in project activities as well as people who provide administrative, logistical, and technical support whose duties require them to access the information, e.g., administrative personnel who prepare and handle project reports. A copy of the roster will be provided to the UTEP Assistant Facility Security Officer (AFSO) in the Office of Research and Sponsored Projects.
e. Access to work sites where classified information is handled or stored may be controlled by badge systems and special locks and entry controls. Such areas will have published access plans that comply with the NISPOM or other sponsoring agency directives.

5.1.3. Visitors.

i. Visitors to classified activities will be appropriately cleared. Visit requests will be submitted by the visitor's parent organization to the UTEP AFSO. Such visits will be conducted in accordance with the NISPOM or other appropriate sponsoring agency directive(s).
ii. Visitors to CUI work sites will be approved by the project Principal Investigator or his/her designee, after appropriate approval of the sponsoring agency's program office, if required. Visitors must have appropriate access and need-to-know, and must be escorted at all times by an approved project staff member; visitors who are directly and routinely involved with the project, e.g., sponsoring agency program office or collaborating organization personnel, do not require escorts.

5.1.4. Personnel.

a. The UTEP Human Resources department should be advised on any job-specific requirements, including citizenship. Job notices will include citizenship requirements, if necessary, and HR will check proof of citizenship of candidates who are not currently UTEP employees. For job candidates who are already in the UTEP personnel system HR may not be able to determine their citizenship based on their personnel files. In those cases where

citizenship is required and HR files cannot document it, the HR department will require the candidate to provide appropriate documentation.

b. All employees of the University are required to pass background checks prior to employment or appointment, including students appointed as research assistants.
c. Students who volunteer to work on research activities without appointments are not subject to background checks. Principal Investigators who consider using such students are responsible to determine citizenship and obtain background checks for suitability as if they would be employed by the University.
d. Employees working on classified activities will have security clearances granted by the appropriate security agency.
e. Citizenship. For activities involving CUI, access is usually restricted to US citizens.
f. Prior to beginning work on a project, all personnel to be granted access to CUI or classified information will sign a non-disclosure statement acknowledging their obligation to safeguard CUI and the penalties for failure to do so.
    i. Persons granted a security clearance will sign the SF 312 (Classified Information Nondisclosure Statement).
    ii. Persons granted access to CUI, employees will sign the UTEP CUI Nondisclosure Statement (Appendix A). They may also be required to sign sponsor-specific forms, such as the DHS Form 11000-6.
g. Subsequent information. If, after a person has been granted access to CUI or classified information, additional or new information comes to light that may raise concerns about his/her suitability for continued access, the individual will be suspended from access immediately pending a final determination by the Principal Investigator, his/her supervisory chain, and the UTEP Assistant Facility Security Officer (AFSO) in the Office of Research and Sponsored Projects, and, in the case of personnel with security clearances, the cognizant security authority. The sponsoring agency will also be notified, so that appropriate actions can be taken to mitigate the risk associated with the inappropriate access. Consult with sponsoring agency directives and project award documents for timeliness requirements for reporting such information.

5.1.5. Work sites.

a. On campus.
    i. When using CUI, authorized users will work in a space that is segregated from unauthorized personnel; a separate room is sufficient. Authorized personnel will know who else has access to the work and will challenge unauthorized others when they attempt to access the site. If unauthorized personnel are present at the work site, CUI will be covered from view. CUI will not be left unattended. When not in use, CUI will be stored as directed in the following paragraph (5.1.6) and the work site will be secured with a locked door.
    ii. Use of classified information is restricted to those areas that adhere to the requirements identified in the NISPOM or the DD form 254 issued by the sponsoring agency.
    iii. Some projects may deal with a mix of non-sensitive and sensitive information and may employ persons who may not have access or need-to-know to work on the latter. The Principal Investigator is responsible to separate the work activities, physically and cognitively, to preclude inadvertent or wrongful disclosure. Those persons authorized to work with CUI will be briefed about the activities and scope of work of the non-sensitive group, and specifically about the limits of information to be exchanged with

the latter. It may be appropriate to explicitly define the specific tasks and limits of the scope of work assigned to the non-sensitive group.

b. Off campus.
   i. At approved sponsor or collaborating agency facilities. Authorized project personnel may visit such facilities in the performance of their duties, subject to the approval of the facility director.
   ii. Other off campus locations. Project personnel may work on CUI at other off campus locations only with the prior approval of the Principal Investigator, and only after appropriate safeguards are applied. Use of classified information is restricted to those areas that adhere to the requirements identified in the NISPOM or the DD form 254 issued by the sponsoring agency.

5.1.6. Storage. When hard copy CUI is not being used it will be stored in a locked container in a locked room; a file cabinet or desk may be sufficient. Key control should ensure that only authorized personnel have access to the room or storage container. Classified information will stored as directed in the NISPOM.

5.1.7. IT Security. CUI may be stored on desk top computers, laptop computers or on university servers, as well as on external memory devices such as hard drives, USB drives, and on CD; password access or encryption will be used at a level appropriate to the sensitivity of the information involved and consistent with the guidance of the sponsoring agency. When not in use, external storage media and laptop computers will be secured in a locked container. Use of classified or export-controlled information on IT systems must adhere to the NISPOM and other relevant regulations. UTEP IT does not restrict information transiting its servers to U.S. only servers managed by U.S. Persons. As such, UTEP Mail service is not adequate for and cannot be used by personnel to transmit or receive export-controlled information. A comprehensive checklist, named UTEP System Security Plan, for assuring compliance exists through the Information Security Office and should be completed in its entirety before receipt of CUI. An example of a System Security Plan is attached as an appendix to this guideline.

5.1.8. Marking. CUI and classified information will be marked in accordance with the sponsoring organization's security directives and the NISPOM and NIST.

5.1.9. Transmission. The transmission or dissemination of CUI or classified information will follow the procedures of the sponsoring organization's security directives and the NISPOM.

5.1.10. Disposition, retention and/or disposal. Disposition and retention of classified material are normally included in the security guidance provided by the DD 254. If this is not the case, UTEP will contact the sponsoring agency for guidance. Destruction will be conducted in accordance with the requirements of the NISPOM. For CUI, the PI will consult with the sponsoring agency's program officer for guidance.

6. Technology Control Plans

6.1 The purpose of a Technology Control Plan (TCP) is compliance with federal regulations to ensure that the transfer of export controlled items, software, or technology, classified information or other CUI data (e.g., For Official Use Only (FOUO), Naval Nuclear Power Information (NNPI)) is not to be conveyed in any manner to foreign national visitors, employees, and students beyond that which is

approved for export by a license or other approval from the appropriate U.S. federal agency, or which is authorized to an individual possessing the required security classification and "need to know." Disclosure of classified information to foreign persons in a visitor status is considered an export disclosure under the International Traffic in Arms Regulations (ITAR) and requires a Department of State license or DoS approval of either a Technical Assistance Agreement or a Manufacturing License Agreement. To delineate and inform employees and visitors of the controls necessary to ensure that no transfer of classified defense information or CUI (defined as technical information or data or a defense service as defined in ITAR paragraphs 120.9 & 120.10) occurs unless authorized by DoS' Office of Defense Trade Controls (ODTC), and to ensure compliance with NISPOM 2-307 and 10-509. The TCP details the export control classification, restriction on release of information, physical and information security protocols, project personnel requirements, annual certification, and closeout procedure. ORSP and AFSO will monitor project related activity throughout the life of the TCP and the Principal Investigator or designated TCP Custodian will be required to disposition all controlled items before close out of the TCP.

6.2 Projects or programs requiring TCPs will coordinate with the UTEP AFSO to implement a plan that is acceptable to the sponsoring agency or the VPR when the activity is UTEP-initiated. A TCP template is available through UTEP ORSP.

7. Responsibilities

7.1 The UTEP AFSO is the proponent for the Information Protection Policy and is responsible to:

a. Promulgate University policy
b. Periodically review project security procedures
c. Provide general training concerning information protection
d. Maintain file copies of project access rosters and security procedures/plans.
e. Other duties as required by the NISPOM and/or sponsoring agency award documents or other directives.

7.2 Principal Investigators are responsible for their projects and to:

a. Determine, as necessary, what elements of information are CUI and/or classified (normally using DoD-provided classification guides for the latter). Review manuscript drafts, website postings, brochures, presentations materials (video, slides, posters, etc.), technology transfer information, and all other information that may be disclosed to the public or persons without a need-to-know, to preclude inclusion of CUI or classified information.
b. Maintain an up-to-date access roster of all people authorized access to project CUI and/or classified information. A current roster will be provided to the UTEP AFSO within the Office of Research and Sponsored Projects.
c. Develop project specific security plans, TCP, that include procedures for access control, worksite control, and safeguards for project CUI and/or classified information.
d. Provide project-specific security training for project personnel.
e. Report violations of security procedures and/or adverse information about project personnel to the AFSO.
f. Other duties as required by the sponsoring agency.

7.3 Senior project personnel, normally co-PIs, will assist the Principal Investigator as he/she directs.

7.4 Persons granted access share in the collective responsibility to safeguard CUI and/or classified information. They will be aware of the project access list and will deny access of unauthorized

personnel to project information and restricted worksites. All are responsible for reporting violations of security procedures and adverse information about project personnel to the Principal Investigator and the AFSO. All personnel granted access to CUI or classified information will sign a non-disclosure statement acknowledging their obligation to safeguard such information and the penalties for failure to do so. Persons granted a security clearance will sign the SF 312 (Classified Information Nondisclosure Statement). For projects dealing with CUI, employees will sign the UTEP CUI Nondisclosure form (Appendix A) unless they are required to sign a sponsor-specific form.

8. Reporting Violations or Security Concerns

8.1 Divulging CUI or classified information to the public or unauthorized personnel constitutes a serious breach of the obligations of the University and project personnel, and may constitute grounds for professional discipline, termination of employment, and civil or criminal prosecution, depending on the nature of the disclosure. The University will cooperate fully with any law enforcement actions. Further, intentional disclosure of designated CUI or classified information without authorization may result in forfeiture of federal research funding and termination of affected programs or projects.

8.2 Principal Investigators must notify the UTEP Assistant Facility Security Officer (ASFO) as soon as possible after discovery of any accidental or intentional disclosure of designated CUI or classified information. The University will in turn notify the sponsoring agency program officer as appropriate.

9. Training

9.1 All personnel authorized access to CUI and/or classified information will receive initial and annual training on these policy guidelines and appropriate sponsoring organization security directives.

10. Flow-through

The requirements of these policy guidelines and any Vice President for Research directive will flow down to all sub-awards or sub-contracts that involve classified or controlled unclassified information. If the sub-awardee does not have an Information Protection Policy or wishes to forgo their own plan then it will comply with this document. If the sub-awardee has an Information Protection Policy it will provide a copy to the UTEP AFSO for review; UTEP reserves the right to impose additional requirements as necessary to ensure compliance with sponsoring agency requirements.

ON BEHALF OF THE VICE PRESIDENT FOR RESEARCH

Nathaniel V. Robinson, P.E.
Assistant VP for Research
Assistant Facility Security Officer
February 27, 2016

Controlled Unclassified Information Nondisclosure Statement

1. I am working on or in support of a project or activity that involves, or may involve, Controlled Unclassified Information (CUI) as defined in the UTEP CCUI Policy Guidelines.
2. I have read and understand the UTEP Classified and Controlled Unclassified Information Policy Guidelines and will comply with same.
3. I have received an initial security briefing by the UTEP AFSO and/or the project Principal Investigator or designee concerning the nature and protection of CUI, including the procedures to be followed in ascertaining whether other persons have been approved for access to it; and I understand these procedures.
4. I have also been briefed about the sponsoring agency requirements contained in its award documentation and/or other directives.
5. I am aware of my responsibilities to:
   a. Safeguard CUI,
   b. Report unauthorized disclosure or dissemination of CUI and any violations or breaches of project security to the UTEP AFSO.
6. I have worked with the UTEP Information Security Office to generate a System Security Plan or have been shown to be excluded.
7. I will comply with all applicable UTEP policy including but not limited to all manuscript drafts, website postings, brochures, presentations materials and technology transfer information. Further, I am aware of and will comply with any sponsoring agency restrictions or requirements concerning publication and/or dissemination of information developed as a consequence of this project.

_____
Printed Name

_____ _____
Signature Date

Witnessed by a supervisory investigator or UTEP VPR designee: I acknowledge that this document was signed in my presence by the person whose name is affixed hereto, and that such person is either a program/project participant or has substantive administrative or support responsibilities that merit his/her acknowledgement of the UTEP CCUI Policy Guidelines and other appropriate rules, regulations policies, procedures and directives.

_____
Printed Name of witness

_____ _____
Signature of witness Date

The University of Texas at El Paso
CUI Checklist to facilitate adherence to Policy Guidelines for
Controlled Unclassified Information (CUI)

Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended. Refer to UTEP Policy Guidelines for Classified and Controlled Unclassified Information and the government's overarching requirements in NIST SP 800-171.

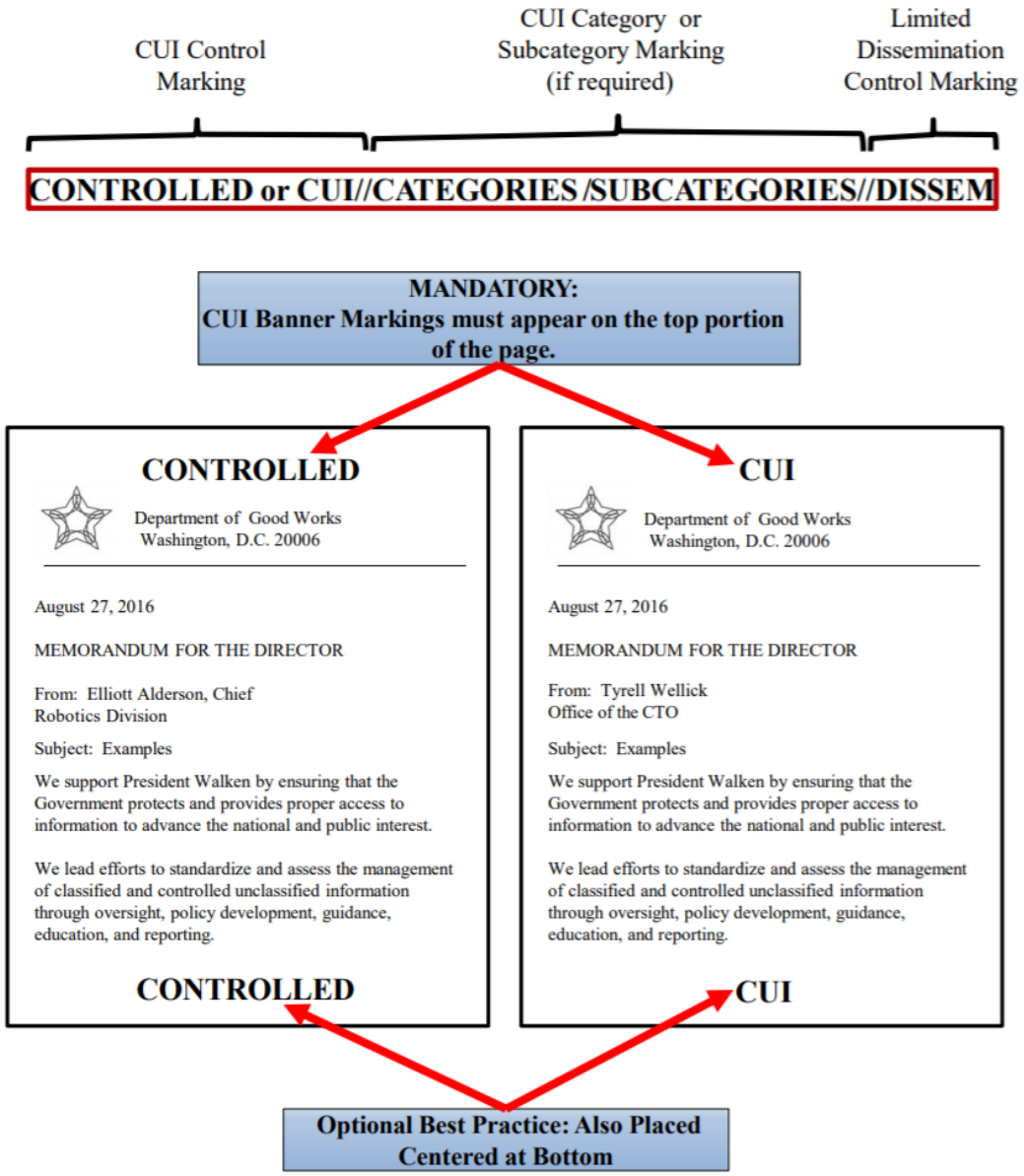
☐ Government sponsor or contractor has properly provided marked Controlled Unclassified Information (CUI). Markings alert holders to the presence of CUI and, when portion markings are used, identify the exact information or portion that needs protection. Markings can alert holders to any CUI dissemination and safeguarding controls.

- ☐ 1. Identify and implement a UTEP System Security Plan for controls to strictly limit access to data and data systems to only those individuals affiliated with the research project and the need for data access. This should include physical control access, storage of media and assets containing CUI, and electronic information systems, including proper destruction of media containing CUI. Contact: Jerry Cochrane gdcochrane@utep.edu
- ☐ 2. Identify and maintain an inventory of personnel who have access to data and information systems relative to the CUI and research. Ensure a unique account per user for authenticating.
- ☐ 3. Ensure all personnel (research, administrators, technicians, etc.) are informed of the security risks associated with CUI, their activities, and methods for mitigating those risks. Ensure each person receives UTEP CUI training and signs the Controlled Unclassified Information Nondisclosure Statement. Contact: Nate V Robinson, nvrobinson@utep.edu
- ☐ 4. Document and maintain an inventory of data and information handling systems and security configuration settings.
- ☐ 5. Create and maintain processes for managing the lifecycle of the information systems used to support the project.
- ☐ 6. Implement a system audit controls to record and report data access, including any anomalous events, with special notion and handling for those deemed unlawful, unauthorized, or otherwise inappropriate to the research.
- ☐ 7. Report incidents according to UTEP policy: contact Nate V Robinson, nvrobinson@utep.edu
- ☐ 8. Conduct screening activities (i.e., background checks) when recruiting personnel for intended access to CUI and ensure access is removed if and when a person is off-boarded or commits a known felonious act.

☐ 9. Conduct periodic audits of all safeguards and policies (physical and cyber) to ensure compliance and safekeeping of CUI, with a document containing date of audit, findings, any incidents and/or anomalies.

☐ 10. Ensure all of the above are documented with the processes for safeguard CUI during research and handling operations documented in an Information Protection Plan, delivered to UTEP FSO: nvrobinson@utep.edu, including updates to personnel rosters as they occur.

Marking:



The University of Texas at El Paso

Information Security Office

SYSTEM SECURITY PLAN

1.0 SYSTEM IDENTIFICATION

1.1 System Name/Title: [State the name of the system; spell out acronyms]

1.1.1 System Categorization: Moderate Impact for Confidentiality

1.1.2 System Unique Identifier: [System Unique Identifier-Will be designated by CISO]

1.2 Responsible Organization:

Name:	The University of Texas at El Paso
Address:	500 W. University Avenue
	El Paso, TX 79968
Phone:	

1.2.1 Information Owner (Government point of contact responsible for providing and/or receiving CUI):

Name:	
Title:	
Office Address:	500 W. University Avenue
	El Paso, TX 79968
Work Phone:	
e-Mail Address:	

1.2.1.1 System Owner (assignment of security responsibility):

Name:	
Title:	
Office Address:	500 W. University Avenue
	El Paso, TX 79968
Work Phone:	
e-Mail Address:	

1.2.1.2 System Security Officer:

Name:	Gerard D. Cochrane Jr.
Title:	Chief Information Security Officer
Office Address:	500 W. University Avenue
Work Phone:	(915) 747-6324
e-Mail Address:	gdcochrane@utep.edu; security@utep.edu

1.3 General Description/Purpose of System: What is the function/purpose of the system? [Provide a short, high-level description of the function/purpose of the system.]

1.3.1 Number of end users and privileged users: [In the table below, provide the *approximate* number of users and administrators of the system. Include all those with privileged access such as system administrators, database administrators, application administrators, etc. Add rows to define different roles as needed.]

Roles of Users and Number of Each Type:

Number of Users	Number of Administrators/ Privileged Users

1.4 General Description of Information: CUI information types processed, stored, or transmitted by the system are determined and documented. For more information, see the CUI Registry at https://www.archives.gov/cui/registry/category-list. [**Document the CUI information types processed, stored, or transmitted by the system below**].

2.0 SYSTEM ENVIRONMENT

Include a detailed topology narrative and graphic that clearly depicts the system boundaries, system interconnections, and key devices. (Note**:** *this does not require depicting every workstation or desktop*, but include an instance for each operating system in use, an instance for portable components (if applicable), all virtual and physical servers (e.g., file, print, web, database, application), as well as any networked workstations (e.g., Unix, Windows, Mac, Linux), firewalls, routers, switches, copiers, printers, lab equipment, handhelds). If components of other systems that interconnect/interface with this system need to be shown on the diagram, denote the system boundaries by referencing the security plans or names and owners of the other system(s) in the diagram.
[Insert a system topology graphic. Provide a narrative consistent with the graphic that clearly lists and describes each system component.]

2.1 Include or reference a **complete and accurate** listing of all hardware (a reference to the organizational component inventory database is acceptable) and software (system software and application software) components, including make/OEM, model, version, service packs, and person or role responsible for the component. **[Insert the reference/URL or note that the hardware component inventory is attached.]**

2.2 List all software components installed on the system. **[Insert the reference/URL or note that the software component inventory is attached.]**

2.3 Hardware and Software Maintenance and Ownership - Is all hardware and software maintained and owned by the organization? **[Yes/No - If no, explain:]**

3.0 REQUIREMENTS

(Note: The source of the requirements is NIST Special Publication 800-171, dated December 2016)

Provide a thorough description of how all of the security requirements are being implemented or planned to be implemented. The description for each security requirement contains: 1) the security requirement number and description; 2) how the security requirement is being implemented or planned to be implemented; and 3) any scoping guidance that has been applied (e.g., compensating mitigations(s) in place due to implementation constraints in lieu of the stated requirement). If the requirement is not applicable to the system, provide rationale.

3.1 Access Control

3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.3 Control the flow of CUI in accordance with approved authorizations.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.6 Use non-privileged accounts or roles when accessing nonsecurity functions.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.7 Prevent non-privileged users from executing privileged functions and audit the execution of such functions.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.8 Limit unsuccessful logon attempts.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.9 Provide privacy and security notices consistent with applicable CUI rules.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.10 Use session lock with pattern-hiding displays to prevent access and viewing of data after period of inactivity.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.11 Terminate (automatically) a user session after a defined condition.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.12 Monitor and control remote access sessions.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.14 Route remote access via managed access control points.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.15 Authorize remote execution of privileged commands and remote access to security-relevant information.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.16 Authorize wireless access prior to allowing such connections.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.17 Protect wireless access using authentication and encryption.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.18 Control connection of mobile devices.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.19 Encrypt CUI on mobile devices and mobile computing platforms.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.20 Verify and control/limit connections to and use of external systems.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.21 Limit use of organizational portable storage devices on external systems.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.22 Control CUI posted or processed on publicly accessible systems.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.2 Awareness and Training

3.3.1 Ensure that managers, systems administrators, and users of organizational 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 those systems.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.3.2 Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.3.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.3 Audit and Accountability

3.3.1 Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.3.2 Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.3.3 Review and update logged events.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.3.4 Alert in the event of an audit logging process failure.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.3.5 Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.3.6 Provide audit record reduction and report generation to support on-demand analysis and reporting.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.3.7 Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.3.9 Limit management of audit logging functionality to a subset of privileged users.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.4 Audit and Accountability

3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.4.3 Track, review, approve or disapprove, and log changes to organizational systems.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.4.4 Analyze the security impact of changes prior to implementation.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.4.6 Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.4.7 Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.4.8 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.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.4.9 Control and monitor user-installed software.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.5 Identification and Authentication

3.5.1 Identify system users, processes acting on behalf of users, and devices.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.5.2 Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.5.3 Use multifactor authentication19F for local and network access20Fto privileged accounts and for network access to non-privileged accounts.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.5.4 Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.5.5 Prevent reuse of identifiers for a defined period.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.5.6 Disable identifiers after a defined period of inactivity.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.5.7 Enforce a minimum password complexity and change of characters when new passwords are created.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.5.8 Prohibit password reuse for a specified number of generations.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.5.9 Allow temporary password use for system logons with an immediate change to a permanent password.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.5.10 Store and transmit only cryptographically-protected passwords.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.5.11 Obscure feedback of authentication information.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.6 Incident Response HERE

3.6.1 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.6.2 Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.6.3 Test the organizational incident response capability

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.7 Maintenance

3.7.1 Perform maintenance on organizational systems.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.8 Media Protection

3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.8.2 Limit access to CUI on system media to authorized users.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.8.4 Mark media with necessary CUI markings and distribution limitations.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

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.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.8.7 Control the use of removable media on system components.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.8.9 Protect the confidentiality of backup CUI at storage locations.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.9 Personnel Security

3.9.1 Screen individuals prior to authorizing access to organizational systems containing CUI.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.9.2 Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.10 Physical Protection

3.10.1 Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.10.2 Protect and monitor the physical facility and support infrastructure for organizational systems.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.10.3 Escort visitors and monitor visitor activity.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.10.4 Maintain audit logs of physical access.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.10.5 Control and manage physical access devices.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.10.6 Enforce safeguarding measures for CUI at alternate work sites.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.11 Risk Assessment

3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.11.3 Remediate vulnerabilities in accordance with risk assessments.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.12 Security Assessment

3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.12.4 Develop, document, and periodically 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.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13 System and Communications Protection

3.13.1 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.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.3 Separate user functionality from system management functionality.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.5 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.6 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.10 Establish and manage cryptographic keys for cryptography employed in organizational systems.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.13 Control and monitor the use of mobile code.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.15 Protect the authenticity of communications sessions.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.16 Protect the confidentiality of CUI at rest.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.14 System and Information Integrity

3.14.1 Identify, report, and correct system flaws in a timely manner.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.14.2 Provide protection from malicious code at designated locations within organizational systems.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.14.3 Monitor system security alerts and advisories and take action in response.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.14.4 Update malicious code protection mechanisms when new releases are available.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.14.5 Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.14.6 Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.14.7 Identify unauthorized use of organizational systems.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

4.0 RECORD OF CHANGES

Date	Description	Made By: