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

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

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 Some of the labels or legacy markings used to describe *sensitive but unclassified information* are:

- For Official Use Only (FOUO)
- Controlled Unclassified Information (CUI) (originally used only for terrorism-related information)
- 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*** rather than *sensitive* information.

(a) 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: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 In the absence of guidance or sponsoring agency directions, principal investigators of University research programs must be attuned to the nature of controlled unclassified information. When such information is acquired or generated through university program activities, even unintentionally or inadvertently, it must be safeguarded in accordance with this policy. Questions should be addressed to UTEP Assistant Facilities Security Officer in ORSP.

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 law, regulations, and government-wide policies. (This excludes all information that is classified under EO 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 sensitive. (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 *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.

3.8 *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 UTEP desires to protect its right to publish the results of University-based research. External sponsors and the University recognize that researchers may work in areas and develop knowledge that may be sensitive. 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 advisable.
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.

a. 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.
b. 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 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 award documentations for timeliness requirements for reporting such information.

5.1.5. Work sites.

a. On campus.
    a. 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 and the work site will be secured with a locked door.
    b. 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.
    c. 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.
   a. 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.
   b. 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 information on IT systems must adhere to the NISPOM and other relevant regulations.

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

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 to describe specific procedures covering HOW access to classified and controlled unclassified information, export controlled information pursuant to the Export Administration Regulations (EAR), or the International Trafficking in Arms Regulations (ITAR) will be controlled in circumstances when foreign nationals are located at facilities as visitors or employees.

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, when the activity is UTEP-initiated, the VPR.

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).
b. Maintain and up-to-date access roster of all people authorized access to project CUI and/or classified information.
c. Develop project specific security plans 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 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.

FOR THE VICE PRESIDENT FOR RESEARCH

Robert M. Currey
Assistant VP for Research
April 13, 2012

Appendix A

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 will comply with all applicable UTEP policy including but not limited to, all manuscript drafts, website postings, brochures, presentations materials (video, slides, posters, etc.), and technology transfer information discussing or presenting data and/or information generated as a direct consequence of participation in this project will be reviewed to preclude the inclusion of CUI. 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