Policy Title: Controlled Unclassified Information Policy	**Policy Number:**
Date Issued: August 22, 2022	**Responsible Executive: Chief Information Officer**
Date Last Revised: August 22, 2022	**Responsible Office: Information Technology Services**

Controlled Unclassified Information Policy

Policy Statement

Baylor University ("Baylor" or the "University") receives federally sponsored grants that access or engage with Controlled Unclassified Information (CUI). This policy does not replace other policies but adds security requirements on top of other policies.

Reason for the Policy

The purpose of the policy is to ensure the compliance with Federal laws and regulations governing the use of CUI. This policy outlines the requirements for receiving, collecting, developing, handling, storing, processing, sharing, and maintaining information that is identified as CUI.

Individuals/Entities Affected by this Policy

This policy applies to all active members of the University community, including faculty, staff, students, vendors, and affiliates who receive federally sponsored funding that requires CUI protection and confidentiality.

Exclusions

Any member of the University community that is not associated with federally sponsored programs that require CUI protection and confidentiality.

Related Documents and Forms

NONE

1. Controlled Unclassified Information Policy

University Policies and Documents

Technology Usage Policy
Employee Personal Information
Handling of Confidential Information
Network Usage Policies
Password Policies
Server Security Policy
Technology Incident Reporting Policy
Data Classification Guide

Other Documents

National Institute of Standards and Technology (NIST) 800-171
32 CFR 2002 Control Unclassified Information Final Rule
CUI Registry: List of Categories of CUI
Executive Order 13556
CUI Markings Handbook
DFARs 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting

Definitions

These definitions apply to terms as they are used in this policy.

Controlled Unclassified Information (CUI)	CUI is government created or owned information that requires safeguarding or dissemination controls consistent with applicable laws, regulations, and government wide policies.
National Institute of Standards and Technology (NIST)	NIST is a special framework designed to safeguard Controlled Unclassified Information (CUI).
Control	An action that is part of your job or policy to protect the safety and integrity of the CUI data and/or environment in accordance with policies, regulations, and laws. Controls contain the following attributes: • Description of the action or policy • Control owner – person responsible for maintaining the effectivity and efficiency of the control • Frequency of the control operation – annually, quarterly, monthly, weekly, daily, or as needed • The control owner will be responsible for producing evidence to prove the effectivity of the control operation in regard to the frequency of the control The controls and the evidence of the controls will be produced when requested for an internal or external control review.

Contacts

Subject	Contact	Telephone	Office email/web site
Support	ITS Help Desk	254-710-4357	https://www.baylor.edu/its/index.php?id=44608

2. Controlled Unclassified Information Policy

Responsibilities

Chief Information Officer	The Chief Information Officer has the responsibility of overseeing the technical CUI environment.
Vice President & Chief Human Resources Officer	The Vice President & Chief Human Resources Officer has responsibility of overseeing the human resource requirements for the CUI environment.
Vice Provost for Research	The Vice Provost for Research has responsibility of overseeing the overall CUI environment.
Individuals with access to CUI environment	Anyone with access to the CUI and/or CUI environment will follow all policies, procedures, federal laws, and regulations.
Control Owner	Person responsible for maintaining the effectivity and efficiency of the control.

Principles

The NIST 800-171 framework describes the fourteen families of security requirements for protecting the confidentially of CUI in University systems. These families consist of 109 controls to address administrative, technical, and operational security controls.

These fourteen security control families include:

- Access Control
- Awareness and Training
- Audit and Accountability
- Configuration Management
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical Protection
- Risk Assessment
- Security Assessment
- System and Communication Protection
- System and Information Security

Sanctions

Sanctions may include, but are not limited to, suspension of technology privileges, termination of employment, referral to Student Judicial Services, a hold on research

funding, disciplinary action, suspension, termination of employment, dismissal from the University, and legal action. Some violations may constitute criminal offenses under local, state, and federal laws. If appropriate, the University will carry out its responsibility to report such violations to the appropriate authorities.

4. Controlled Unclassified Information Policy