UNIVERSITY OF
SOUTH ALABAMA

Responsible Office: Office of Research and Economic Development

Effective: June 25, 2019

Last Revised: June 25, 2019

Next Review: June 25, 2021

Controlled Unclassified Information (Research) Policy

1. Introduction

1.1. Purpose

The University of South Alabama may receive data shared by the federal government or may create data or information as part of sponsored projects or to conduct federal business. This data, information and related documents may be classified as Controlled Unclassified Information (CUI). The University is obligated to ensure that all systems and processes involved with CUI are compliant with National Institutes of Standards and Technology (NIST) standard found in NIST Special Publication 800-171. This policy provides requirements and guidance so individuals in receipt or development of CUI can conduct research or other business in compliance with CUI regulation. Non-compliance may result in fines or the inability to continue receiving Federal funds associated with the use of this data whether directly received from the government or indirectly through associated covered contracts and contractors.

1.2. Applicability

This policy applies to all data that is classified as CUI as well as any technology, system, service, network, department, or personnel that transmit, process, or store CUI. It covers transmission of data and information that is transmitted in any manner, including electronic and paper. This policy applies whether the network connections are remote (cloud) or campus-based.

1.3. Scope

Any person, school, college, or department who handles CUI on behalf of the University must abide by this policy.

2. Definitions

NIST Special Publication 800-171

NIST Special Publication 800-171 is a Federal standard that standardizes security controls applied to CUI and systems and processes involved with this data within federally-funded environments.

Controlled Unclassified Information (CUI)

Controlled Unclassified Information is any information in any form that law, regulation, or government-wide policy requires having safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.

Environment

Environment is defined as the systems upon which CUI resides and the physical infrastructure that houses these systems. Examples might be an individual research lab consisting of a room with desktop computers housing CUI or a student records system residing on multiple servers within a cabinet in a datacenter. The room(s) or area(s) housing the computer systems along with the computer systems themselves define the environments to which this policy applies.

NIST 800-171 Controls

The NIST 800-171 framework consists of 110 elements covering administrative, technical, and operational security controls designed to focus on protecting the confidentiality of unclassified-but-controlled information. Those controls are: 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 Communications Protection, and System and Information Security

Compensating Controls

A compensating control, also called an alternative control, is a mechanism that is put in place to satisfy the requirement for a security measure that is deemed too difficult or impractical to implement at the present time. Compensating controls for a NIST 800-171 requirement need to mitigate the underlying risk that the requirement is designed to address. The Office of Information Security will work with the parties responsible for environments that are involved with CUI to design and approve compensating controls.

3. Policy

This policy provides requirements and guidance for all use of CUI for the University of South Alabama. These are the minimum requirements for securing CUI - other applicable requirements still apply as well. All environments involved with CUI must comply fully with the NIST 800-171 standards (either directly or through compensating controls).

4. Procedures

4.1 Departments and individual users must take actions to protect CUI from unauthorized disclosure and follow the requirements as specified in NIST 800-171.

4.2 All environments that are involved with CUI must undergo an annual NIST 800-171 compliance assessment before interacting with CUI.

4.2.1 These assessments will result in an attestation report signed by the Director of Information Technology Risk and Compliance or designee.

4.2.2 The assessment results will be reported to the Vice President of Research & Economic Development for research-related activities.

4.2.3 Any items of non-compliance found during the assessment must be remediated before any interaction with CUI is allowed.

4.3 A periodic risk assessment to organizational operations, assets, and individuals, resulting from the operation of information systems and the associated processing, storage, or transmission of CUI. Assessments will be performed by the Director of Information Technology Risk and Compliance.

4.4 All environments that are involved with CUI must also operate in a manner that allows incident reporting within 72 hours of cyber incidents involving CUI.

5. Responsible Position/Enforcement

Policy - Vice President for Office of Research and Economic Development

Policy Enforcement – Director of Information Technology Risk and Compliance

6. Related Documents

6.1 References

NIST Special Publication 800-171
DFARS 252.204-7012