t

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)

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.