Controlled Unclassified Information

Type of Policy: Administrative

Effective Date: August 2018

Policy Owner: Information Technology Services Security

Contact Name: James Hunter

Contact Title: Information Security Officer

Contact Email: JamesHunter@clayton.edu or itsecurity@clayton.edu

Reason for Policy:

NIST Special Publication 800-171 (NIST 800-171), is a Federal standard that standardizes security controls applied to Controlled Unclassified Information (CUI) and systems and processes involved with this data within federally funded environments. Clayton State is obligated to ensure that all systems and processes involved with CUI are compliant with NIST 800-171 to continue receiving Federal funds associated with the use of this data (either directly received from the government or indirectly through associated covered contracts and contractors).

Policy Statement:

This approval process applies to all activities involving the use of CUI:

All environments (see definitions section) involved with CUI must comply fully with the NIST 800-171 standards (either directly or through compensating controls) and follow the guidance provided by the Clayton State System Security Plan (Clayton State SSP). Any deviations from the Clayton State SSP must be approved by the Information Security Officer (ISO). The ISO will route such request to the CIO, as appropriate, for additional approval.

All environments that are involved with CUI must undergo an annual NIST 800-171 compliance assessment by Cyber Security before interacting with CUI. These assessments will result in an attestation report signed by the ISO, or designee. The assessment results will be reported to the Clayton State CIO. Any items of non-compliance found during the assessment must be remediated before any interaction with CUI is allowed. All environments that are involved with CUI must also operate in a manner which allows incident reporting of cyber incidents involving CUI within 72 hours.

This policy provides requirements and guidance for all use of CUI for Clayton State University. These are the minimum requirements for securing CUI.

Scope:

Anyone who handles CUI on behalf of the Institute must abide by this policy.

Definitions:

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. Information Security will work with units to design and approve compensating controls.
Controlled Unclassified Information (CUI)	Controlled Unclassified Information is any information that law, regulation, or government-wide policy requires to have 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.

Related Information:

Clayton State System Security Plan

NIST Special Publication 800-171