Policy Name	Security Training Policy
Policy Number	50000.045/ CMMC AT.2.057
Effective Date	February 3, 2023
Administrative Division	Division of Academic Affairs
Unit	Department of Information Technology
Revised Date	

NIST SP 800-171 Requirement 3.2.2	**Other Requirements** • CIS Controls v7.1 17.5, 17.6, 17.7, 17.8, 17.9 • NIST CSF v1.1 PR.AT-1, PR.AT-2, PR.AT-3, PR.AT-4, PR.AT-5 • CERT RMM v1.2 OTA:SG4.SP1 • NIST SP 800-53 Rev 4 AT-2, AT-3
CMMC Capability **C012** **Conduct Training**	

1. Policy Statement
Jackson State University's ("JSU" or "University") Division of Information Technology's ("DIT") intention for publishing a Security Training policy for CUI data to ensure all personnel are properly trained to perform their security duties and responsibilities to protect the University's CUI data.

2. Purpose
The purpose of this policy is to implement policies and procedures for granting access to Controlled Unclassified Information (CUI).

3. Scope
This policy applies to all organization workforce members and all systems, network, and applications that process, store or transmit CUI. This policy also applies to all vendors, partners, researchers and contractors.

4. Responsibilities
The Chief Information Security Officer is responsible for ensuring the implementation of this policy.

5. Definitions
5.1. *Controlled Unclassified Information (CUI)* - is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified.

6. Policy
All environments involved with CUI must comply fully with the NIST 800-171 standards (either directly or through compensating controls. Jackson State University and its employees, vendors, and contractors will implement the following:

6.1. Security Training

6.1.1 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities by:

a. Providing Role based Security Training before authorizing access to the information system or performing assigned duties on an annual basis or as needed for new hires, or when required by information system changes.

b. Provide all personnel with the means to provide input and feedback on their skill gaps and their training needs for their assigned information security-related duties and responsibilities.

c. Generate documentation for training(s) attended.

7. Sanctions/Compliance

Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

8. Related Standards, Policies, and Processes

Security Awareness Training

- Information security awareness, education, and training
- Controls against malware

Role-Based Security Training

- Information security awareness, education, and training

9. Revision History

- Policy Created: February 2, 2023