Insert Company Name Or Logo]	
Title: Electronic Data Integrity Control	**P&P #:**
Approval Date:	**Review:**
Effective Date:	**Security Team**

Purpose: To implement the ability to authenticate that transmitted data is protected against unauthorized alteration or destruction during transmission over electronic communications networks.

Scope: This policy applies to all employees and other members of the workforce (whether paid, volunteer, or contractor) working in all facilities under the organization's ownership.

Definitions:

1. Integrity: The property that data or information have not been altered or destroyed in an unauthorized manner.
2. Workforce Member: Employees, volunteers (board members, community representatives), trainees (students), contractors and other persons whose conduct, in the performance of work for [Insert Local Gov/K-12 Name], is under the direct control of [Insert Local Gov/K-12 Name].

Procedure:

1. The Security Officer will approve the electronic mechanisms that will be implemented to protect sensitive and regulated data from unauthorized alteration or destruction and to authenticate the integrity of the data during transmission.
2. The Security Officer will determine the appropriate steps to confirm effective implementation of the integrity controls, to review and update them as necessary as defined by the Information Systems Administrative Control Evaluation policy.
3. The Security Officer will provide affected workforce members with training and awareness regarding integrity controls implemented to protect sensitive and regulated data from unauthorized alteration or destruction during transmission over electronic communications networks.
4. The Security Officer will ensure that actual and potential damage to the integrity of confidential or sensitive information, including ePHI, FERPA, PII, and other sensitive data is appropriately addressed.
5. Transmitting sensitive and/or regulated data via a removable media such as a flash drive or removable hard drive requires the files to be password protected. The receiving entity shall be authenticated before transmission.
6. The IT department shall maintain adequate firewall protection of the network.

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

a. The firewall shall be configured to “deny” rather than “allow” as the default setting.
b. Unused firewall ports shall be closed.
c. IT staff shall examine firewall logs and reevaluate the security configurations periodically (Insert time period/every week, every month, etc.).

7. All encryption mechanisms utilized for transmission of sensitive and regulated data will support a minimum of 1024 bit encryption.

VIOLATIONS:

Any known violations of this policy should be reported to the Security Officer. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with [Insert Local Gov/K-12 Name] procedures, up to and including termination of employment.

[Insert Local Gov/K-12 Name] may advise law enforcement agencies when a criminal offense may have been committed.

Attachments: None

Related Policies: None

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.