[Insert Company Name Or Logo]	
Title: Encryption	**P&P #:**
Approval Date:	**Review:**
Effective Date:	**Security Team**

Purpose:

[Insert Local Gov/K-12 Name] is committed to operating in compliance with all applicable laws, regulations, and policies. We have adopted this policy to outline the security measures required to protect electronic information systems and related equipment from unauthorized use.

The goal of these policies is to protect sensitive and regulated data and other protected information such as personally identifying information by enhancing the security of our electronic information systems. [Insert Local Gov/K-12 Name] requires securing sensitive and regulated data contained on all mobile media, laptops, workstations, servers, and external hosted sites that are not located in approved, secure data centers. Approved Secure Data Centers are defined as data centers that have had a formal, external risk assessment on the physical and logical controls in the last year with no findings that would render the data center unsecured.

Scope:

These policies and guidelines apply to all members of the workforce (whether paid, volunteer or contractor) who use, collect and/or access sensitive and regulated data. These policies and guidelines apply to all [Insert Local Gov/K-12 Name] owned and personal electronic devices that are connected to our networks and receive, store or transmit sensitive and regulated data.

Definitions:

1. Encryption: the process of converting data to an unrecognizable or "encrypted" form.
2. Workforce Member: Employees, volunteers (board members, community representatives), trainees (students), contractors and other persons whose conduct, in the performance of work with regulated data or under the direct control of a department that deals with regulated or sensitive data, whether or not they are paid by such a department or organization.

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.

Procedure:

1. The Information Security Officer will provide appropriate workforce members with training and awareness regarding encryption methods implemented to protect sensitive and regulated data from unauthorized alteration or destruction during transmission over electronic communications networks.
2. All sensitive and regulated data will be encrypted, whether at rest or in transmission, unless a risk analysis indicates that such encryption is not necessary to protect those data. Any risk analysis must consider the probability and criticality of risks to security.
3. All electronic devices that receive, store and/or transmit sensitive and regulated data and are not located in an approved secure data center must use approved encryption methods to secure the information stored on or transmitted outside the secure clinical network.
4. Servers that are not located in an approved secure data center are required to have all information stores of sensitive and regulated data encrypted.
5. Sensitive and regulated data contained on laptops or workstations are required to be either File, Folder or Full Disk Encrypted.
6. If mobile devices (smart phones and tablets) must be allowed to connect to [Insert Local Gov/K-12 Name] internal network, they must be encrypted.
7. External storage media (backup tapes, removable drives, etc.) must be encrypted.
8. Files that contain sensitive and regulated transmitted across the Internet (e-mail attachments sent outside network, or file transfers to other entities) must have the attachments encrypted or use an approved secure encryption method to deliver the information.

Exceptions:

Existing systems and applications containing sensitive and regulated data which cannot use encryption because of a technological limitation, but have compensating controls, may be granted a special exception by the Information Security Officer. However, these systems and applications will be required to have a formal risk assessment performed by the Information Security Officer to ensure that major risks are addressed via compensating controls to protect the data in lieu of encryption. Exceptions will be reviewed periodically and removed when a suitable solution is available.

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

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.

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.