NWF Health Network
Policy & Procedure

Series:	900: Data Collection, Records and Reporting
Policy Name:	Cryptographic and Encryption Controls
Policy Number:	922
Origination Date:	02/22/2024
Regulation:	CFOP 50-4 CFOP 50-5 CFOP 50-13 CFOP 50-14
Referenced:	900-915 x 1 MIS Handbook

Policy

Cryptographic controls must be utilized for sensitive information classified by NWFHN as {PROTECTED} or {RESTRICTED} including, but not limited to: Personally Identifiable Information (PII), Protected Health Information (PHI), credit card numbers, passwords, intellectual property, budget or contract proposals, legal correspondence and research and development information. All encryption mechanisms utilized by NWFHN must be authorized by the appropriate authority.

Users must not attempt to utilize any form of cryptography, including, but not limited to, encryption, digital signatures, and digital certificates, which has not been approved and installed/implemented by our designated representative. The use of all encryption mechanisms must meet relevant regulatory and legal requirements, including any import/export requirements and use of cryptography in other countries. Define the recommended encryption methods - such as AES-128, RSA, Bitlocker, or ECC.

Network Encryption

All sensitive information classified by NWFHN as PROTECTED or RESTRICTED including, but not limited to, PII, PHI, credit card numbers, passwords, and research and development information, must be encrypted when transmitted outside of NWFHN networks. This includes transmission of information via email or other communication channels. Remote management activities for NWFHN, such as contractors accessing our network remotely, must consistently employ session encryption. Define remote access procedures such as using VPN to access corporate systems while teleworking.

Hard Disk Encryption

All sensitive information classified by our company as PROTECTED or RESTRICTED including, but not limited to PII, PHI, credit card numbers, and passwords, must be encrypted. When feasible, hardware encryption must be utilized over software encryption. It is our company's policy to use laptops and desktops that have encrypted hard drives.

Roles and Responsibilities

Responsible Parties.

Our company's leadership and management team are responsible for maintaining and enforcing the policies, standards and guidelines established within this document. Employees, contractors, vendors, service providers, partners, affiliates, and third parties are responsible for ensuring all actions are in accordance with our management policies and objectives.

All users are required to sign our company's Acceptable Use Policy and acknowledge they understand and will abide by the standards and individual responsibilities it defines. All changes to the Acceptable Use Policy are communicated to all staff, contractors and other third parties in a timely fashion.

Ownership

All IT policies, standards, and guidelines are owned, established and managed by the IT Manager (or equivalent authority) within NWFHN.

Communication

All policies, standards and guidelines are available for reference to all company users. The availability of this program will also be communicated to all users annually.

Compliance

All users must comply with our NWFHN's corporate policies. Any user found to be abusing the privilege of using our corporate assets and access to business systems, or not in compliance with any of these policies, may be subject to disciplinary action, up to and including termination of employment.

Applicability

This policy is applicable to all NWFHN employees working both on site and remotely.