

Data Encryption Policy

# Overview/Purpose

This policy sets guidelines for the use of encryption to ensure that **<Utility Name>** can leverage cryptographic software and techniques to safeguard our member data and our operations, while mitigating the attendant risks.

# Scope

This policy shall apply to all uses of encryption within **<Utility Name>**.

# Policy

It is the responsibility of employees, contractors, vendors and agents with access to the network to ensure that confidential data is encrypted at rest and in transit, whenever practical. Confidential data shall be encrypted at rest, and when it leaves the utility’s premises. This includes:

* Databases with PII data or other confidential information accordingly to data classification,
* Laptops and other mobile devices,
* Portable data storage devices,
* Off-site backups.

## Transport layer security

The use of Transport Layer Security is strongly encouraged for all employee and contractor web browsing and for use on web servers. All non-console administration access to cardholder data will require the use of strong transmission encryption. Such data should never be transmitted via end-user messaging technologies, including email and text messages.

**<Utility Name>** web servers should be configured to use most recent TLS, but no earlier than TLS 1.2.

## Database and shared storage device encryption

Databases and shared storage devices such as server, SAN, or NAS disks, shall utilize data encryption either made available by the database vendor, or by using third party solutions. The encryption methodology implemented should meet or exceed the requirements in NIST 800-111, Guide to Storage Encryption Technologies for End User Devices.

## Full disk encryption

Every workstation, laptop and mobile device should have full disk encryption enabled and configured, according to best practices for that platform.

Suspend-to-ram (S3 or “sleep”) shall be disabled for platforms which hold encryption keys in memory while suspended. This includes Windows, Linux and Android operating systems, and excludes Apple OS X and iOS devices as well as Google Chromebooks.

## Procuring secure encryption software

All encryption software used must be approved for use by **<person or department responsible for this policy>**.

Encryption software must be actively supported and audited for security to be eligible for approval. The **<person or department responsible for this policy>** is responsible for determining whether a piece of cryptographic software meets these criteria, and for maintaining a list of approved encryption software.

## Key Management

All secret key material (keys, passphrases, etc.) used by employees and contractors must be stored securely and redundantly. Employees and contractors must submit secret key information to the IT Manager or their designee, for storage in an offline key repository.

Keys shall be stored offline, in a secure location, such as a safe. The offline key repository must not be accessible from a network-connected computer. Access to the repository must be limited to the minimum personnel necessary.

# Compliance

## Compliance Measurement

The <**person or group responsible for policy**> will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

## Exceptions

Any exception to the policy must be approved by the <**person or group responsible for policy**> in advance.

## Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action in accordance with **<Utility Name>** HR policies.

# Related Standards, Policies, and Processes

* Adapted from “Cyber Security Policy Framework”   
  (<https://www.nreca.coop/wp-content/uploads/2015/09/cyber_security_policy_framework.docx>)   
  Cyber Security Policy Framework was created by the Kentucky Association of Electric Cooperatives (KAEC) Information Technology (IT) Association - Cyber Security Subcommittee.
* NIST 800-111, Guide to Storage Encryption Technologies for End User Devices (<http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf>)

# Governance Responsibilities

The ISP uses the RACI model for assigning responsibility.

|  |  |  |  |
| --- | --- | --- | --- |
| Responsible | Accountable | Consulted | Informed |
| IT Manager | **CEO/GM** |  | **All Employees** |

*[Explanatory Note: <Utility Name> should feel free to alter section to reflect the specific responsibility requirement determined by <Utility Name> management.]*

# Approval

\_

<**Insert title of approver**> Date

# Revision History

|  |  |  |
| --- | --- | --- |
| Date of Change(s) | Revised by | Summary of Change(s) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |