Encryption Management Policy

Purpose

The purpose of the (District/Organization) Encryption Management Policy is to establish the rules for acceptable use of encryption technologies relating to (District/Organization) **Information Resources**.

Audience

The (District/Organization) Encryption Management Policy applies to individuals responsible for the set up or maintenance of (District/Organization) encryption technology.

Policy

* All encryption technologies and techniques used by (District/Organization) must be approved by (District/Organization) IT Management.
* (District/Organization) IT Management is responsible for the distribution and management of all encryption keys, other than those managed by (District/Organization) customers.
* All use of encryption technology should be managed in a manner that permits properly designated (District/Organization) personnel to promptly access all data, including for purposes of investigation and business continuity.
* Only encryption technologies that are approved, managed, and distributed by (District/Organization) IT may be used in connection with (District/Organization) **Information Resources**, other than those managed by (District/Organization) customers.
* (District/Organization) IT Management will create and publish the (District/Organization) Encryption Standards, which must include, at a minimum:
  + The type, strength, and quality of the encryption algorithm required for various levels of protection.
  + Key lifecycle management, including generation, storing, archiving, retrieving, distributing, retiring, and destroying keys.
* All (District/Organization) information classified as **confidential** must be encrypted when:
  + Transferred electronically over public networks.
  + Stored on mobile storage devices.
  + Stored on laptops or other mobile computing devices.
  + At rest.
* The use of proprietary encryption algorithms is not permitted, unless approved by (District/Organization) IT Management
* The use of encryption for any data transferred outside of the United States must be formally approved by (District/Organization) IT Management prior to transfer.

Definitions

See Appendix A: Definitions

References

* ISO 27002: 10, 14, 18
* NIST CSF: PR.DS
* (District/Organization) Information Classification and Handling Policy

Waivers

Waivers from certain policy provisions may be sought following the (District/Organization) Waiver Process.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Version History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Modified Date | Approved Date | Approved By | Reason/Comments |
| 1.0.0 | February 2018 |  | SecurityStudio | Document Origination |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |