HEART OF TEXAS WORKFORCE DEVELOPMENT BOARD, INC.

POLICY

ID NO.: HWD CS 019-23	**DATE ISSUED:** 06/01/2023
PROGRAM: Cybersecurity	**KEYWORD:** Data Encryption Policy

SUBJECT: Data Encryption Policy

PURPOSE: To provide staff with information and guidance on data encryption expectations and oversight within the Heart of Texas Workforce Solutions environment.

REFERENCES: Security Control Standards Catalog Texas Department of Information Resources Version 2.0 Effective Date 1/20/22; TWC Information Security Manual v3.0

POLICY: DATA ENCRYPTION POLICY

GENERAL POLICY

Sensitive Organizational data should be retained or handled only when required. Encryption can be an effective information protection control when it is necessary to possess sensitive organizational data.

All organizational employees should understand that data encryption is not a substitute for other information protection controls, such as access control, authentication, or authorization; that data encryption should be used in conjunction with those other controls; and that data encryption implementations should be proportional to the protection needs of the data.

REQUIREMENTS

Transmission: In order to protect the confidentiality and integrity of the Organization's sensitive data; any data classified as **Confidential** data, and having a required need for confidentiality and/or integrity, shall be transmitted via encrypted communication to ensure that is does not traverse the network in clear text. It is further recommended, but not required, that data classified as **Sensitive** be transmitted via encrypted communications when possible.

Storage: In order to protect the confidentiality and integrity of the Organization's sensitive data; any data classified as Confidential data, and having a required need for confidentiality and/or integrity, shall be stored encrypted in systems and/or databases and/or portable media.

A combination of business practices and technology can act as mitigating factors and could significantly reduce the risk of unauthorized data exposure, thereby offsetting the specific need to implement data encryption. Examples of such mitigating factors include, but are not limited to, those identified in APPENDIX-C.

Encryption Services

The symmetric algorithms referenced in APPENDIX-D shall be used for encrypting Confidential information. The algorithms referenced in APPENDIX-E shall be used for public key asymmetric encryption of Confidential information. The encryption services referenced in APPENDIX-F shall be used for digital signature purposes when Confidential information is involved. Digital signatures shall be used to associate a user or entity with a respective public key.

Encryption Key Management

Encryption keys used to protect Confidential data shall also be considered Confidential data. Where symmetric encryption is used to protect Confidential data:

- Master keys shall be changed at least once per year.

When asymmetric encryption is used, the operational period of asymmetric keys associated with a public key certificate are defined by the encryption key management plan of the issuing certificate authority.

Encryption keys are confidential information, and access shall be strictly limited to those who have a need-to-know. The owner(s) of data protected via encryption services shall explicitly assign responsibility for the encryption key management that should be used to protect this data. If keys are transmitted over communication lines, they shall be sent in encrypted form. The exchange of keys should employ encryption using a stronger algorithm than is used to encrypt data protected by the keys.

Encryption keys that are compromised (e.g., lost or stolen) shall be reported immediately to the Information Technology Office. The key shall be revoked, and a new key generated. Key re-assignments shall require re-encryption of the data.

Certificate Authorities

Encryption keys that are generated by the Organization's production certificate authority (CA) and used to control access to the CA server or used by the CA to perform functions shall be stored on Hardware Security Modules (HSM).

CAs must be designed such that all CA administrator functions are accounted for in detail. Ideally, no single administrator shall obtain full access to the CA encryption keys (e.g., separation of duties, dual control, etc.)

APPENDIX A: Application of Encryption for Data Transmission

File Transfers
Encryption of Confidential file transfers can be achieved via the use of an encrypted transmission protocol or network service (e.g., SCP, SFTP, etc.) or by transferring a Confidential file that has been encrypted prior to the transmission.

E-mail
Confidential content transmitted in e-mail messages shall be encrypted prior to the transmission, presented via a secure web application, or encrypted in a secure message format, given e-mail is exposed to the possibility of unauthorized access at points throughout the delivery process.

Interactive Sessions
Encryption of Confidential data, including login passwords, transmitted during remote login sessions (e.g., Telnet, TN3270, and remote software for PCs) shall be provided through secure applications or protocols.

Web-Based Applications
Encryption of Confidential data communicated between a user's browser and a web-based application shall be provided through secure protocols (e.g., HTTPS, TLS/SSL, etc.) The display of Confidential data shall be limited to only what is required by the user's authorized use of the application.

Network Printer Communication
Encryption of Confidential data that is output to a printer connected to a network shall be provided through secure printing applications or protocols to prevent unauthorized network interception.

Remote File Services
Encryption of Confidential data transmitted by remote files services shall be provided through encrypted transmission protocols (e.g., IPsec, ISAKMP/IKE, SSL/TLS) to prevent unauthorized interception.

Database Access
Encryption of Confidential data transmitted between an application server and a database shall be implemented to prevent unauthorized interception. Such encryption capabilities are generally provided as part of, or an option to, the database server software.

Application-to-Application Communications
Encryption of Confidential data transmitted between cooperating applications shall be provided through commonly available encrypted protocols (e.g., SOAP with HTTPS) to prevent unauthorized interception.

Virtual Private Network (VPN)
A VPN connection offers an additional option to protecting Confidential data transmitted via the network when other alternatives are not feasible. The use of VPNs should be carefully considered so that all security and networking issues are understood. IT staff should be consulted prior to any VPN implementations.

APPENDIX B: Applications of Encryption for Data Storage

Whole Disk Encryption
Encryption of Category I data stored on portable computing devices (e.g., PDAs, tablet PCs, laptops, and smart phones), as well as storage media, (e.g., CDs, DVDs, and USB drives) shall be provided through a whole disk encryption tool or one that can at least be configured to encrypt all Confidential data.

File Encryption
Encryption of Confidential data shall be provided to facilitate the secure transport of individual files over a network without transmission encryption or to off-line storage devices (e.g., CDs, DVDs, or USB drives.)

Database Storage
Encryption of Confidential data contained in a database server shall be provided through whole disk encryption or through features native to the database server software. Encryption capabilities native to database server software may allow for encryption of specific tables or columns of a database and may also be required to segregate access rights among multiple applications that utilize a single database server.

APPENDIX C: Examples of Potential Mitigating Factors

- Firewall Restricting Capabilities
- Detailed Audit Logging
- Detailed Process Logging
- Intrusion Detection Capabilities
- Intrusion Prevention Capabilities
- Integrity Checking Capabilities
- Separation of Sensitive Duties
- Physical Security Capabilities

APPENDIX D: Symmetric Algorithms

- AES (128, 192, or 256 bit)
- RC6 (256 bit)
- Serpent (128, 192, or 256 bit)
- Twofish (128, 192, or 256 bit)

APPENDIX E: Public Key Asymmetric Algorithms

- RSA (minimum 1024 bit)
- ECC (minimum 384 bit)

APPENDIX F: Digital Signature Algorithms

- RSA (minimum 1024 bit) with SHA-2
- DSA (minimum 2048 bit) with SHA-2
- ECDSA (minimum 384 bit) with SHA-2

DOCUMENT CONTROL

Document Name	Data Encryption
Document Control Number	
Document Identification	Version 1.0
Owner/Approver Identification	Cybersecurity Coordinator
Author	Matilda Alonzo
Document Reviewer(s)	HOTWDB ITSSC
Review Plan	This document should be reviewed by all parties on a regular basis. Next Review is 5/24/2024
Latest Version	1.0
Distribution	The master version of this document is stored in <Storage Location>. PRINTED COPIES OF THIS DOCUMENT ARE FOR REFERENCE ONLY!

REVISION HISTORY		
Date	Revised By	Changes
<Release Date>	<Author>	Initial Release