`

COST: **$$**$$ IMPACT: **HIGH** COMPLEXITY: **MEDIUM**

2.L: Does the WWS use encryption to maintain the confidentiality of stored sensitive data?
Recommendation: Do not store sensitive data, including credentials (i.e., usernames and passwords) in plain text.

Why is this control important?

See Factsheet 2.K for a description of the importance of general encryption.

This control is important, as attackers will often attempt to break into computer systems and databases to steal sensitive information and "case" the network for a future attack. Additionally, many ransomware cyberattacks also include extortion attempts whereby the attacker will steal a WWS's sensitive data and threaten to expose it on the Internet if a ransom is not paid. If the WWS encrypts data, the attacker will not be able to use it if stolen as it will be unreadable.

Implementation Tips

Only allow access by authorized users.

Update any weak or outdated data encryption software.

Resources

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: See control SC-13 (page 308) and SC-28 (page 317) for more information on "Cryptographic Protection" and "Protection of Information at Rest". *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

NIST Policy Template Guide: See Encryption Standard (4.2) Data at Rest SOP for encryption that can be included in the utility's cybersecurity policy. *https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp2089.pdf*

Additional Guidance

- ✓ A WWS can implement encryption for stored data using BitLocker for drive encryption of servers and clients (desktops and laptops), as well as with Transparent Data Encryption (TDE) for database files. A WWS can encrypt and password-protect individual sensitive files in Windows by right-clicking a file, selecting Properties -> Advanced -> "Encrypt contents to secure data". Cloud services for remote storage and application hosting will likely offer this capability by default.
- ✓ To securely store and use credentials, a WWS can use a password management software (e.g., LastPass, 1Password) or other account management method. Password management software securely stores credentials, reduces the difficulty of remembering passwords, and simplifies the use of complex passwords.

`

Microsoft Core Infrastructure Guide: See the links below for instructions on how to encrypt stored data via BitLocker Drive Encryption, Transparent Data Encryption (TDE) for databases, and individual file encryption. *https://learn.microsoft.com/en-us/dynamics365/business-central/dev-itpro/security/transparent-data-encryption*;

https://learn.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview;

https://support.microsoft.com/en-us/windows/how-to-encrypt-a-file-1131805c-47b8-2e3e-a705-807e13c10da7