Encrypt Data at Rest

Any data that is not being actively transferred can be referred to “data at rest.” This includes data residing on hard drives, USB sticks, and with third-party cloud service providers. Encryption allows for data at rest to be properly secured. For instance, encrypting personally identifiable information (PII) with strong encryption algorithms protects the data from accidental disclosure in the case of a data breach.

Elections offices may maintain a number of systems that must use encryption and are responsible for identifying data that should be encrypted.

In modern laptops, desktops, and server environments, encryption capabilities of some form are often built into the software and hardware stack. These capabilities may be enabled by default or will need to be properly configured. Third-party encryption utilities may also be needed to encrypt specific data, such as within an application, database, or a USB device.

Goals

1. Enable encryption for laptops, desktops, servers, and mobile devices, known as full-disk encryption (Level 1 maturity)
2. Encrypt backups (Level 1 maturity)
3. Encrypt removable devices, where practical, such as with USB devices (Level 2 maturity)

Actions

For Encrypt Data at Rest, the necessary actions vary by maturity as detailed below.

Level 1 Maturity

1. Enable encryption, often called full-disk encyrption, on all devices that have encryption technologies built into the device.
   - You can use the Level 1 maturity Asset Protection worksheet as a template to track your work.
   - The cost effective tools section below may help, depending on the types of systems you have in your environment.
2. Encrypt backups. Use the backups best practice as a guide.

Level 2 and Level 3 Maturities

Organizations operating at a Level 2 or Level 3 maturity should take additional actions, including:

1. Work with those who provide IT infrastructure, whether vendors or your own IT staff, to implement encryption for all sensitive data.
2. Implement encryption when data is at rest (e.g., stored in a database or on a device) and in transit (e.g., sending through email) and ensure all encryption meets your election office’s adherence to encryption standards.

The National Institute of Standards and Technology (NIST) Special Publication 800-175B provides the U.S. federal requirements for encryption standards to secure data at different sensitivity and classification levels.

NIST Special Publication 800-122 provides the U.S. federal requirements for protecting the confidentiality of personal information.

Cost-Effective Tools

- GCA Cybersecurity Toolkit for Elections: Update Your Defenses: A toolbox with links to free tools relevant to this best practice
- Bitlocker: Built-in encryption for supported Microsoft® Windows devices.
- FileVault: Built-in encryption for MacOS devices.
- Veracrypt: Open-source, free full disk encryption utility.
- EaseUS: This free program can encrypt system images.

Mapping to CIS Controls and Safeguards

- 3.6: Encrypt Data on End-User Devices
- 3.9: Encrypt Data on Removable Media
- 3.11: Encrypt Sensitive Data at Rest
- 11.3: Protect Recovery Data

Mapping to CIS Handbook Best Practices

- 4, 12, 84