

SecureAge

SecureAge SecureDocument Media



In this digitally connected age, the access of electronic documents has been made a lot simpler. Employees or outsiders can view and gain access to their company's documents anytime and anywhere. As an Executive Leader, you have a right to be concerned. Unauthorised viewing and distribution of confidential customer data, key financial records, employee information and other sensitive documents can spell disaster.

Such unauthorized access to confidential information can result in serious repercussions like lost revenue, violations of privacy laws and legislation, unfair advantage in purchasing and hiring decision, diminished customer confidence and many more. How then can you protect your sensitive documents from unauthorised viewing?

How do you protect your sensitive documents?

To protect your sensitive documents, you should always follow these 3 guidelines:

1) Encrypt your document files

Encryption can protect documents from unauthorised viewing in event of you losing your data. Encryption makes data unreadable except to authorised users who have the required "key" installed on their computer.

2) Set policies and assign different level of file permissions

You can restrict who can view or change a document by setting policies to control. You can grant permissions or deny access to a document (or any computer resource).

3) Use SecureDocument Media, Secure Digital Rights Management for Portable Devices

SecureAge Digital Rights Management (DRM) is a proven platform that allows you to send sensitive electronic documents to third party securely. It allows the user to protect electronic documents with expiry date deliver content for playback on computers, portable devices, and network devices.

With SecureDocument Media, you can:

- Protect sensitive electronic documents with an expiry date.
- Protect sensitive electronic documents with read-once or allowable read count.
- Permanently destroy sensitive electronic documents automatically upon expiry or zero read count.
- Track and provide audit trail with timestamp and error logs.

Key Features

Protect Sensitive Electronic Documents

- Enable sending of highly sensitive electronic documents to third party.
- Allow Users to protect highly sensitive electronic documents with an expiry date.
- Allow Users to protect highly sensitive electronic documents with read-once or any allowable read count.
- Ensures that all highly sensitive documents are permanently destroyed upon expiry or zero read count.
- Provides Tracking and Audit Trail with timestamp and error log.

Provides 2-Factor Security

- PKCS#11 Standard Compliance.
- Supports Smart Card and USB tokens.
- Double Protection with the thumbdrive volume and files are encrypted using user's certificate.

Provides Secured Volume Encryption

- Support PKI authentication.
- Provides maximum security with full thumbdrive encryption using 256-bit AES encryption.
- Provides seamless and transparent access upon successful user authentication.

Provides Full Strength File Encryption

- Support PKI encryption and decryption.
- Protects highly sensitive electronic documents with file-level 256-bit AES encryption.
- Provides automatic file encryption, including all temporary files.
- Provides automatic file decryption when reading files from thumbdrive directly.

Prevents Data Leak

- Protects and hide highly sensitive electronic documents from non-trusted processes including Windows Explorer.
- Permanently destroy highly sensitive electronic documents upon tampering.
- Allows applications white-listing enabling only trusted processes to read the documents.
- Trusted applications are independently run from the secured volume.
- Prevents saving of highly sensitive electronic documents to local/network drive.
- Prevents and disable Printscreen Hot key Function.

No Proprietary Hardware

- Simple to implement, using standard U3 thumbdrive.
- No need to access server or internet for DRM Control.