# *Users Quick Reference to Get Started with Dell Data Guardian v2.8*

This Quick Reference provides a brief introduction of Data Guardian and tips for finding information in the *User Guide*.

## Purpose of Data Guardian

Based on policy set by your administrator, you can encrypt many file types. Only authorized users have access. Your data is secure at rest and when in motion:

- Personal email account
- Removable media
- Cloud-based file sharing system
- Network file share

Data Guardian can be installed on Windows, Mac, or as mobile apps on Android or iOS. If your enterprise uses Data Guardian web portal, you can view encrypted files or grant access for others to view a file on a device without installing a Data Guardian client.

## Options with Data Guardian

Data Guardian has a wide range of options. Your administrator will tell you which apply to your enterprise. See the *Data Guardian User Guide* > Chapter 1 for a list of options. Here are some examples:

You may have one or more of these options:

- **Basic File Protection** – non-Office applications and file extension types (for example, Notepad with **.txt**).
- **Protected Office documents** (**.docx, .pptx, .xlsx, .docm, .pptm, .xlsm, .pdf**)
  - **Opt-in** mode – you can determine which documents to protect.
  - *or*
  - **Force-Protected** mode – higher level of security. Files are swept and encrypted.
- Tamper detection (Windows, Mac, mobile, web)
- Data Classification, TITUS classification, Encryption for Outlook email (Windows)
- **Cloud Encryption** – Data stored in the cloud is encrypted. (Mac, mobile, web)

## All Users – Before you begin

You must know:

- The encryption options for your enterprise and the level of security.
- Additional policies that impact security.
- Cloud storage provider to use – if the enterprise has a preferred provider. (Mac, mobile, web portal)

Data Guardian supports these environments. When installing, note items that you may be prompted for and have them available:

- Hosted (Windows, Mac, and mobile) – An Installation ID (Only for multi-tenant.)
- On-prem (Windows, Mac, and mobile) – Fully qualified host name of the Dell Server (Required to install.)
- Workspace One and MSI environment (Windows only and on-prem)

**Important** – When first installing Data Guardian, be aware that some or all files may be encrypted. Make backups. A Data Guardian Recovery tool exists for the administrator to recover and decrypt files, but Dell recommends making a backup.

## Internal Users – Install on Windows

Here are additional tips for Windows. You must be a local administrator on the computer. See **Chapter 3** of the *Data Guardian User Guide*.

After you install:
In the notification area, confirm that the Data Guardian icon has a green checkmark.

### Install on Other Operating Systems

See the *Data Guardian User Guide*:

- **Mac** – See **Chapter 6**.
- **Android or iOS** – v See **Chapter 7**.
- **Web portal Mac** – See **Chapter 8**.

### Reminders/Tips for Protected Documents

Your administrator will tell you which options apply to your enterprise.

- For an overview of options, see the *Data Guardian User Guide* > Chapter 1.
- For *Basic File Protection*, see the *Data Guardian User Guide* > Chapter 4.
- For *Protected Office Documents*, see the *Data Guardian User Guide* > Chapter 4.

If Data Guardian encrypts a document and you open it on a device that does not have Data Guardian, only a cover page displays. An unauthorized user cannot view your data.

### Reminders/Tips for Cloud Encryption

You can use Cloud Encryption with Mac, mobile, or web portal.

- Chapter 5 has information on each cloud sync client that relates specifically to Data Guardian.
- With Opt-in mode (but not Force-Protected mode), a *Secure Documents* folder as added at the root of the *Documents* folder. Office documents in this folder are encrypted.

### Share Files with External Users

An internal user can share secure files with an external user through email, network share, or removable media. To grant access to an external user, right-click a local file and select *Protected File Access*. For more information, see the *Data Guardian User Guide > Chapter 9*.

### Cover Pages on Encrypted Documents (Windows, Mac, Mobile, web portal)

Based on policy, if you send an encrypted file to an unauthorized external user, a cover page displays stating that this is a protected document.

Based on policy, you or your administrator can grant access to the file and provide a valid email address for them.

A policy allows your administrator to customize the information on the cover page and provide links where the unauthorized user can register and gain access to the encrypted file.

The cover page also provides links for installing Data Guardian on an Android or iOS mobile device, or using it with web portal. The external user must first register with a valid email.