HOW-TO GUIDE:

# GILISOFT FULL DISK ENCRYPTION FOR LAPTOPS

Windows 7, 8, XP, Vista and 2000

## Foreword

The data stored on BMS laptop hard drives typically contain PII (personally identifiable information). To prevent third parties from accessing this data in the event of theft or loss, laptop hard drives must be encrypted as mandated by the Handbook.

Encryption is a way of scrambling the data on a hard drive, so that, if the drive is lost or stolen, the data on that drive cannot be retrieved by anyone else. Your password/key is the way to unscramble that data, and needs to be safeguarded. If you are to lose that password, it is similar to losing the keys to a vault, you will lock yourself out, and nobody will be able to retrieve the data.

So when you think of encryption, *backup, backup, backup* should come to mind. Did we mention *backup*? Solely backing up to an external drive that is encrypted is risky. The encryption software can cause the external drive to fail (it does not matter what product you use - free or paid), the external drive itself could stop working, or the password may get lost or forgotten. In all 3 scenarios, you could lose all of your data, most notably:

- CaseLink data.
- Chapter 7-related documents received through PACER or third parties, or any document you create and save to your hard drive.
- Non-Chapter 7-related data or documents saved to your hard drives.
- Email you push to your computer from an external source.

BMS strongly suggests employing an IT professional to create a disaster recovery plan before you find yourself in this situation.

At the very minimum, utilizing an online backup solution on a regular basis for all of your data (especially that described above) should be part of your disaster recovery plan. Make sure to back up your data and test restore from that backup ***before*** you begin encrypting the data on your drives.

Encryption **does not protect your computer from being corrupted by malware from the Internet.** It is your responsibility to be aware of where you're browsing as viruses can come from just about anywhere on the Internet. Be sure to keep your system software and browsers properly updated (patched) and use the appropriate antivirus software to protect your computer.

This is a general guide to encrypt your laptop using the GiliSoft Full Disk Encryption.

Installing GiliSoft takes less than 10 minutes to set up/complete; however, the actual time it takes to encrypt a drive takes 3-4 hours in most cases, but could take in excess of 8+ hours.

**WARNING: Make sure you have performed a full backup of your system and tested doing a restore of your data from the backup before attempting to encrypt.**

## Installation Instructions

1. **Purchase, Download and Install** – Copy and paste the following BMS-client specific URL in your web browser to purchase the GiliSoft encryption software at a 40% discount:
   https://shopper.mycommerce.com/checkout/cart/add/21821-15?ss_coupon=GILI-NIJN-LAWR
   Follow the instructions provided on this site to download and install the GiliSoft software on your system.

2. **Create a bootable rescue disk (LiveCD):**

   Prior to encrypting your data, it is strongly recommended that you create a bootable rescue disk (LiveCD) with GiliSoft Full Disk Encryption on a CD or DVD disk. The LiveCD rescue disk will allow you to gain access to data in case of any emergency if the computer fails to boot while also allowing you to access and decrypt your data.

   Step 1: Obtain the LiveCD image file from support@gilisoft.com

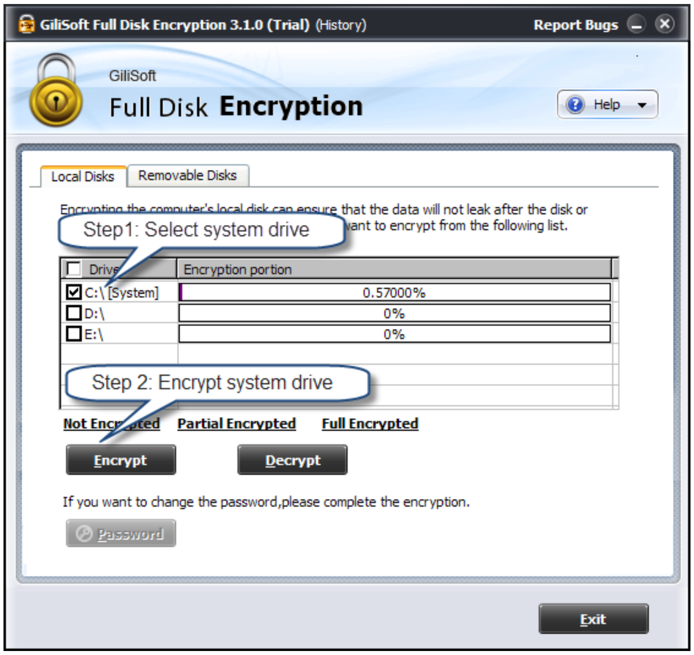
   Step 2: Burn it into a CD/DVD.

3. **Encrypt Your Data:**

   Step 1: Once you have completed steps 1 & 2 above, **launch the GiliSoft Full Disk Encryption software**.

   Step 2: **Select the system drive**, as shown below.

   Step 3: **Click the 'Encrypt' button** and **input a password** to start encrypting your laptop.



GiliSoft Full Disk Encryption 3.1.0 (Trial) (History)

Encrypting the computer's local disk can ensure that the data will not leak after the disk or

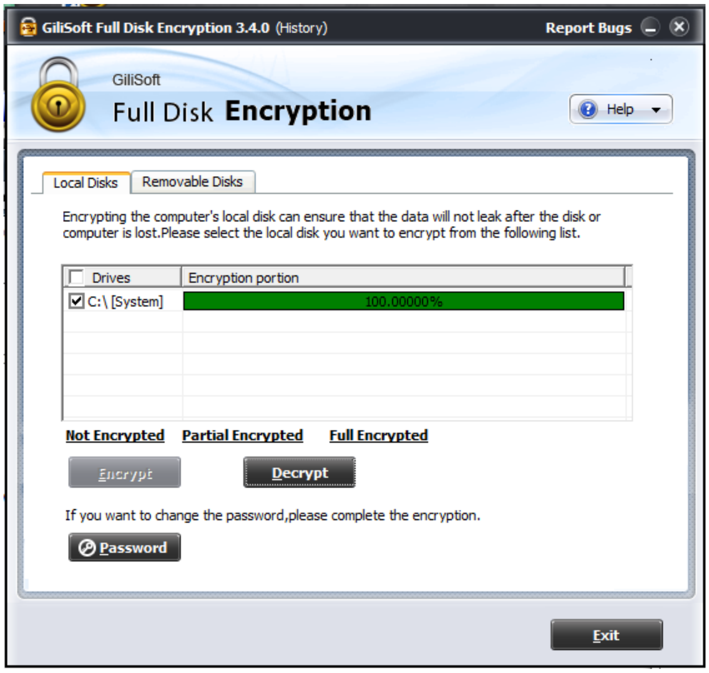
want to encrypt from the following list.

| ☐ Drive | Encryption portion |
|---|---|
| ☑ C:\ [System] | 0.57000% |
| ☐ D:\ | 0% |
| ☐ E:\ | 0% |

If you want to change the password,please complete the encryption.

The actual time it takes to encrypt a drive takes 3-4 hours in most cases, but could take in excess of 8+ hours. **Make sure that your laptop is fully charged and plugged into a charger.** BMS recommends that you **start your encryption process at the end of the day** so that your data can be fully encrypted overnight.

The following is a screenshot of a fully encrypted drive.



Encrypting the computer's local disk can ensure that the data will not leak after the disk or computer is lost.Please select the local disk you want to encrypt from the following list.

| □ Drives | Encryption portion |
|---|---|
| ☑ C:\ [System] | 100.00000% |

If you want to change the password,please complete the encryption.

Either click **'Exit'** or perform any other necessary functions such as encrypting external drives (covered in the BMS How-to Guide: *GiliSoft Full Disk Encryption for External Drives* – distributed separately).