# Table of Contents

1 ABOUT THIS GUIDE ......................................................................................................................................... 3
   1.1 WHO SHOULD USE IT.................................................................................................................................... 3
   1.2 TYPOGRAPHICAL CONVENTIONS .................................................................................................................... 4

2 INTRODUCTION ................................................................................................................................................ 5
   2.1 PURPOSE ..................................................................................................................................................... 5
   2.2 SYSTEM REQUIREMENTS ............................................................................................................................... 6
   2.3 BEFORE INSTALLATION .................................................................................................................................. 6
   2.4 SCOPE ......................................................................................................................................................... 7
   2.5 SOFTWARE ORGANIZATION ........................................................................................................................... 8

3 INSTALLING THE SOFTWARE ........................................................................................................................ 9
   3.1 INSTALLING ENCRYPTION PLUS® HARD DISK ................................................................................................. 9
   3.2 STARTING YOUR COMPUTER AFTER INSTALLATION ....................................................................................... 32

4 FREQUENTLY ASKED QUESTIONS ................................................................................................................ 33
1 About this guide

This document is divided into the following chapters:

Chapter 1, “About this Guide.”

Chapter 2, “Introduction” gives an overview of the key features, system requirements, notes to read prior to installation, software scope, and software organization.


Chapter 4, “Frequently Asked Questions” provides answers to common questions about the software.

1.1 Who Should Use It

This guide is intended for laptop and PC users who store sensitive data on the hard drive:

This guide assumes that you have some knowledge security standards and data encryption.
1.2 Typographical Conventions

This document uses the following typographical conventions:

Command and option names appear in bold type in definitions and examples. The names of directories, files, machines, partitions, and volumes also appear in bold.

Variable information appears in italic type. This includes user-supplied information on command lines.

Screen output and code samples appear in monospace type.

In addition, the following symbols appear in command syntax definitions.

Square brackets [ ] surround optional items.

Angle brackets < > surround user-supplied values.

Percentage sign % represents the regular command shell prompt.

Pipe symbol | separates mutually exclusive values for an argument.

Denotes where to click
2 Introduction

2.1 Purpose

The purpose of this document is to provide step-by-step instructions for the installation and use of Guardian Edge Secure Encryption for the hard disk drive.

- Guardian Edge is a software application that assists in the encryption of the hard drive of a Microsoft Windows-based laptop or PC. In the event that a laptop or PC is lost or stolen, hard drive encryption prevents unauthorized access to data stored on the hard drive.

- The intended audiences of this software are University of Louisville faculty and staff laptop or PC users who may have sensitive information stored on the hard drive, especially those in health sciences profession who may access or store protected health information.
2.2 System Requirements

- Operating Systems
  - Windows 2000 Server, Service Pack 4 (SP4)
  - Windows XP Professional Edition, Service Pack 1 (SP1)
  - Windows XP Professional Edition, Service Pack 2 (SP2)
  - Windows 2003 Server, Service Pack 1 (SP1)
  - Windows 2003 Server, Service Pack 2 (SP2)
  - Windows Vista (Ultimate, Enterprise, Business)

**Note:** It is strongly advised that you make a current backup of the data stored on your hard drive on the university network (I drive) or another storage device such as a USB, or “thumb”, drive.

**Note:** Guardian Edge Hard Disk® Encryption does NOT support 64-bit Windows.

**Note:** If your computer has two monitors, your machine may contain two video cards, a primary card and a secondary card. The primary video card should be disabled before installing this software. It is recommended that you work with your Tier 1 for technical assistance with this issue.

**Note:** For full encryption functionality, it is best to install on a machine that is connected to the University of Louisville network.

- Hardware
  - Pentium III processor or better
  - 800x600 minimum video resolution
  - 16-bit color
  - 40 MB of hard disk space

2.3 Before Installation

Before installing Encryption Plus® Hard Disk:
- Make a current backup of the data stored on your hard drive using the university network (I drive) or another storage device such as a USB, or “thumb”, drive.
- Due to the length of time it takes for the program to finish it is recommended that you allow for the encryption process to run overnight.
- Complete any operating system version upgrades.
- Complete all partitioning, formatting and resizing.
If you are connected to a network, disable any file sharing or other network services that offer remote access to data stored on your computer.

**Note:** Do not interrupt installation process by shutting down or powering off your computer.

### 2.4 Scope

- Encryption Plus® Hard disk encryption protects your laptop or PC in two ways:
  - It requires you to authenticate prior to logging in to Windows. This prevents unauthorized users from accessing your hard drive.
  - It encrypts your data. This means that your data is unreadable to anyone who does not have proper authority to access or read information on your hard drive.

- Once you have authenticated to Encryption Plus® Hard Disk, your data is not protected so it is recommended that you maintain the laptop or PC security measures you currently use:
  - Maintain a current backup of data stored on your hard drive.
  - Always run current virus protection software on your laptop or PC.
  - Always enable the password-protected Windows screensaver if you are stepping away from your desktop PC.
  - Never leave your laptop unattended, even if it is only for a short time.

- You must shut down your laptop or PC to be fully encrypted by Encryption Plus® Hard Disk.

**Note:** Any documents or data that are open and in use prior to your machine going into “sleep” or “hibernate” mode are unencrypted.
2.5 Software Organization

This document applies to:

- Guardian Edge Encryption Plus® Hard Disk Windows 2000, XP, and Vista
- Abbreviated EP Hard Disk
- Version 7.2.0
3 Installing the Software

3.1 Installing Encryption Plus® Hard Disk

1. In your web browser, go to http://louisville.edu/it/itechxpress to download or order a CD.

2. Double click the executable file entitled hdd_encrypt. If you are a Windows Vista user, continue to step 3. If you are a Windows XP user, go on to step 4.

3. You will receive a User Access Control window. Click Allow.

Note: This step is for Vista users only.
4. The **Program Window** will open and run in the background during setup.

**Note:** Do not close this window during installation.
5. The **Welcome** window for the InstallShield Wizard for Encryption Plus® Hard Disk will also open. Click **Next**.
6. At the **License Agreement** window, read the license agreement. **Click I accept the terms in the license agreement.** Then **Click Next.**
7. At the **Destination Folder**, **Click Next**.
8. At the **Ready to Install the Program** window, click **Install**.

---

**Note:** The installation process should not be interrupted. Do not power off your machine at this time.
9. The **Installing Encryption Plus Hard Disk** window will show the progress of the installation using the **Status** bar.
10. The **Install Shield Wizard Completed** window will appear. Click **Finish**. If you are a Windows Vista user, continue to step 11. If you are a Windows XP user, go on to step 12.
11. You will receive a **User Access Control** window. Click **Allow**.

**Note:** This step is for Vista users only.
12. The **Welcome to the InstallShield Wizard for Encryption Plus Management Console Client** window will appear. **Click Next.**

**Note:** This is the second phase of the installation process. It is not a repeat of the initial installation. Please continue as instructed.
13. At the License Agreement window you will be asked to accept an additional license agreement. 

Click I accept the terms in the license agreement. Then Click Next.
14. At the **Destination Folder**, **Click Next**.
15. At the **EP Management Console Client – Create Folder** window, **Click Yes** to create a new folder for Guardian Edge Console Client.

![EP Management Console Client - Create Folder](image-url)
16. At the **Ready to Install the Program** window, **Click Install**.
17. The **Installing Encryption Plus Management Console Client** window will show the current progress of the installation using the **Status** bar.
18. At the **InstallShield Wizard Completed** window, Click **Finish**.

![InstallShield Wizard Completed](image)

The InstallShield Wizard has successfully installed Encryption Plus Management Console Client. Click Finish to exit the wizard.
19. A **Restart Your System** window will ask you to restart your computer. **Click Yes.**

**Note:** Make sure you save your data and close all open programs prior to restarting your computer.
20. When you restart your computer you will see Encryption Plus Hard Disk – Setup Required window. Click OK.
21. You will now see the **Encryption Plus Hard Disk Welcome** window. **Enter** and **Confirm** your **EP Hard Disk User Name**. **Enter** and **Confirm** your **EP Hard Disk Password**. **Click Next**.

**Note:** You will use this user name and password each time you log on to your computer.
22. On the **Encryption Plus Hard Disk Authenti-Check** window you are required to **Enter Answers** to three personal security **Questions**. The answers to these questions are used to identify you in the event you have lost your password. You will have to supply both the **Question** and **Answer** to question three. Once you have entered the requested information, **Click Next**.

**Note:** Keep your answers simple by using a one-word answer consisting of either all uppercase or all lowercase letters.
23. On the **Encryption Plus Hard Disk Encrypt Drives** window, **Check Box C** under **Partition**. Then, under **Initial Encryption Speed**, **Check** either **Fast** or **Slow**. Click **Next**.
24. The status bar on the **Encryption Plus Hard Disk Encrypt Drives** window shows the **Percentage Complete** of the encryption process. Depending upon the speed of your processor, the size of your hard disk, and whether you chose the slow or fast option, the encryption process could potentially take up to 10+ hours.

**Note:** On average, the encryption process will most likely take between 2.5 to 4 hours for most users. You may continue to work on your PC while the hard disk is encrypting. You may click the hide button if you wish; this will close the box, but the process will still run in the background.

**Note:** Do not interrupt the installation process by powering off your computer.
25. Once your encryption process is complete, the **Encryption Plus Hard Disk Encryption Complete** window will appear. Congratulations! Your computer’s hard drive is now encrypted. **Click Hide** to close this window.

**Note:** Encryption Plus® Hard Disk will now run as an icon in the system tray at the bottom of your computer screen.

Encryption Plus Hard Disk will continue to protect your drives. This application will always run in the background on your system.

You can adjust settings and review the encrypted status of local drives using the navigation tabs above.

For further assistance, including step-by-step instructions, click the Help button.

To return EP Hard Disk to the status area, click Hide.
3.2 Starting Your Computer after Installation

1. Start your PC as you normally would.

2. Guardian Edge Encryption Plus® Hard Disk will automatically run when you start your computer. When starting your computer you will see the Welcome window. Press Enter.

3. Next you will be prompted to authenticate. Enter your User Name and Password. Press Enter. You will then go through the Windows login process to finish starting your computer.

Note: Use the Tab key to navigate from the User Name field to the Password field.
4 Frequently Asked Questions

1. Will running full disk encryption increase the risk of a hard drive failure on my laptop or PC?
   
   No. Encryption Plus® Hard Disk will not increase the risk of a hard drive failure.

2. If there is an installation corruption, will I be able to recover the encrypted data?
   
   Yes. Encryption Plus® allows for data recovery in the case of installation corruption.

3. Will running full disk encryption slow down my laptop or PC?
   
   No. Encryption Plus® Hard Disk will not slow down your computer’s performance.

4. Can I stop running antivirus software on my laptop or PC now that my data is encrypted?
   
   No. Encryption Plus® Hard Disk is an added layer of security and is not meant to replace any security measures you currently use with your laptop PC.

5. Can I stop applying Windows patches on my laptop or PC now that my data is encrypted?
   
   No. Encryption Plus® Hard Disk is an added layer of security and is not meant to replace any security measures you currently use with your laptop PC.

6. Now that my data is encrypted, is it necessary to lock laptop or PC when I am away from it?
   
   Yes, you should always lock your laptop or PC when you are away from it. Once you have signed into your computer using your Encryption Plus® Hard Disk user ID and password, the data becomes unencrypted to enable you to access it. The data does not become encrypted again until you shut down your computer.
7. Will I be able to put my laptop or PC into “hibernate” mode once I have installed Encryption Plus® Hard Disk?
   Yes. Encryption Plus® Hard Disk will still allow your laptop or PC to “hibernate”

8. Will I be able to defragment my laptop’s or PC’s hard drive once it is encrypted?
   Yes. Encryption Plus® Hard Disk works seamlessly with all standard Windows maintenance tools.

9. Can I encrypt my computer if it is running a 64-bit operating system?
   No. At this time Encryption Plus® Hard Disk does not support 64-bit Windows.

10. What if my computer has two monitors?
    If your computer has two monitors, it may contain two video cards, a primary card and a secondary card. If this is the case you will need to contact your Tier 1 or the Help Desk to disable the primary video card.

11. Who do I contact for help?
    Contact your department’s Tier 1 or the HelpDesk. You can reach the HelpDesk by phone at 852-7997 or on the web at http://louisville.edu/it/helpdesk.