2022

Protecting Information and Data Guide

UNIVERSITY ADVANCEMENT

Protecting Information, Data and Devices Guide

Updated: 2.10.2022

Contents

Introduction

Protecting Information and Data at Western is critical in an age where information is used as currency. This includes all information systems, computers, and computing equipment, owned by and/or operated by or on behalf of the University, as well as data owned by and /or operated by or on behalf of the University whether that data is accessed or used on University-owned equipment or on personal devices

Information and Data Defined

Information and Data includes, but is not limited to, emails, data lists, reports, presentations, strategies, ideas, and hardware. Essentially any work by the University that is not made publicly available.

Storing and Sharing Information and Data

There are two forms managed by Information Management that are related to storing and sharing information and data.

1. **Request for Access Form** – STAFF MEMBERS
   - The Request for Access form must be signed by all staff in order to access CRM and any University data
   - The Request for Access form can be found @ advhelp.westernu.ca, by clicking on the grey block titled Security/Access
   - The signed form should be scanned and sent to the Information Management team at avimcore@uwo.ca. Only when this form is received, can access to CRM be granted
   - After signatures are redacted, the form is uploaded to the CRM system on the employee's constituent profile. It can be found on the Documentation and Interactions tab, on the Constituent Documentation sub-tab.

2. **Non-Disclosure Agreement** – VOLUNTEERS
   - Volunteers must sign a Non-Disclosure Agreement prior to any University data being released
   - The NDA form can be found @ advhelp.westernu.ca within the grey block titled Security/Access
   - The signed form should be scanned and sent to the Information Management team at avimcore@uwo.ca.
   - After signatures are redacted, the form is uploaded to the CRM system on the volunteer's constituent profile. It can be found on the Documentation and Interactions tab, on the Constituent Documentation sub-tab.
   - Note: Lists related to Commemorative Giving do not require a Non-Disclosure Agreement from the families to release donor info (name, address) for thank you letters as directed by the Commemorative giving team.

The availability of these documents in a central location (CRM) allows visibility for all areas of University Advancement to confirm the forms are signed and that release of data is possible going forward.

There are two methods supported by Western to store and share information.

1. **External Share Drive (W Drive)**
   - For instructions to access the External Share drive click HERE.
   - Note that access rights must be granted to you before following these instructions.

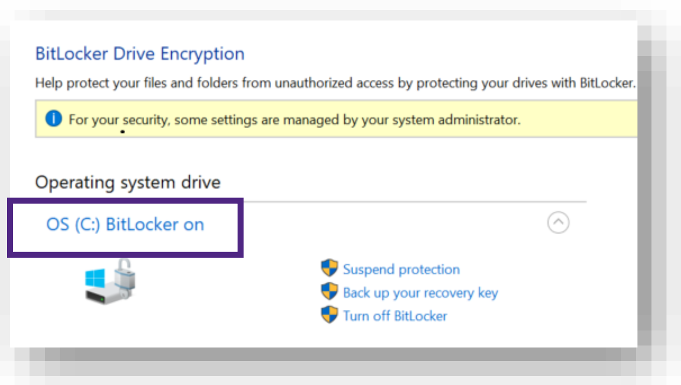
2. **OneDrive**
   - For instructions for how to access OneDrive click HERE.
   - To learn how to use OneDrive, visit the Office 365 support page by clicking HERE.
   - The signed form should be scanned and sent to the Information Management team at avimcore@uwo.ca

Security and Maintenance

Encrypt your laptop/computer

Your work computer or laptop should be encrypted in case it is lost or stolen. Follow these steps to ensure your laptop or computer is encrypted.

1. **Check to see if your laptop is encrypted:**
   - In the search box on the taskbar, type **Manage BitLocker** and then select it from the list of results. (Note: You'll only see this option if BitLocker is available for your device.)
   - If your laptop or computer **IS** encrypted, it will read **OS (C:) BitLocker on**



BitLocker Drive Encryption

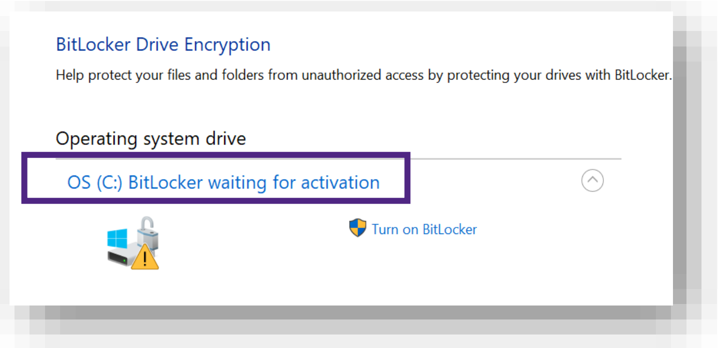
Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

For your security, some settings are managed by your system administrator.

Operating system drive

OS (C:) BitLocker on

- If your laptop or computer **IS NOT** encrypted, it will read **BitLocker waiting for activation**



BitLocker Drive Encryption

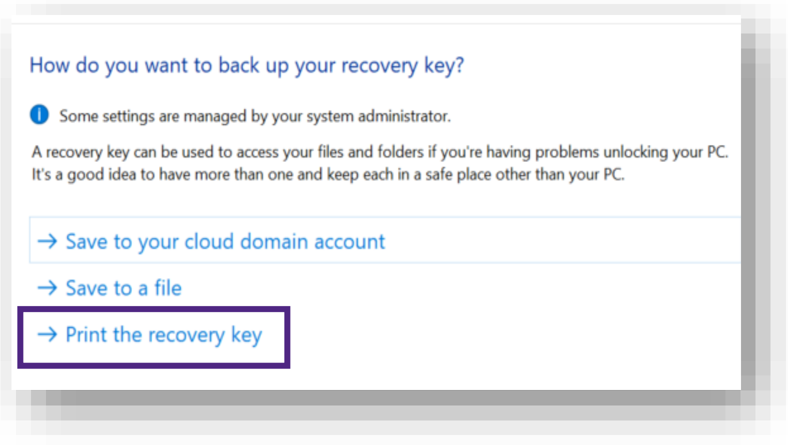
Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

OS (C:) BitLocker waiting for activation

2. **Encrypt your laptop or computer:**

- To encrypt click **Turn on BitLocker**
- From the available options click **Print recovery key**

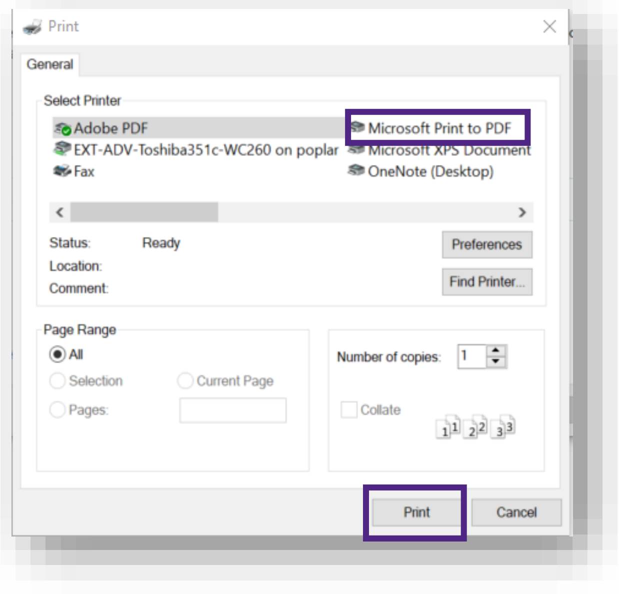


How do you want to back up your recovery key?

Some settings are managed by your system administrator.

A recovery key can be used to access your files and folders if you're having problems unlocking your PC. It's a good idea to have more than one and keep each in a safe place other than your PC.

- Under the heading Select Printer, click on **Microsoft Print to PDF**
- Click **Print**



Status: Ready

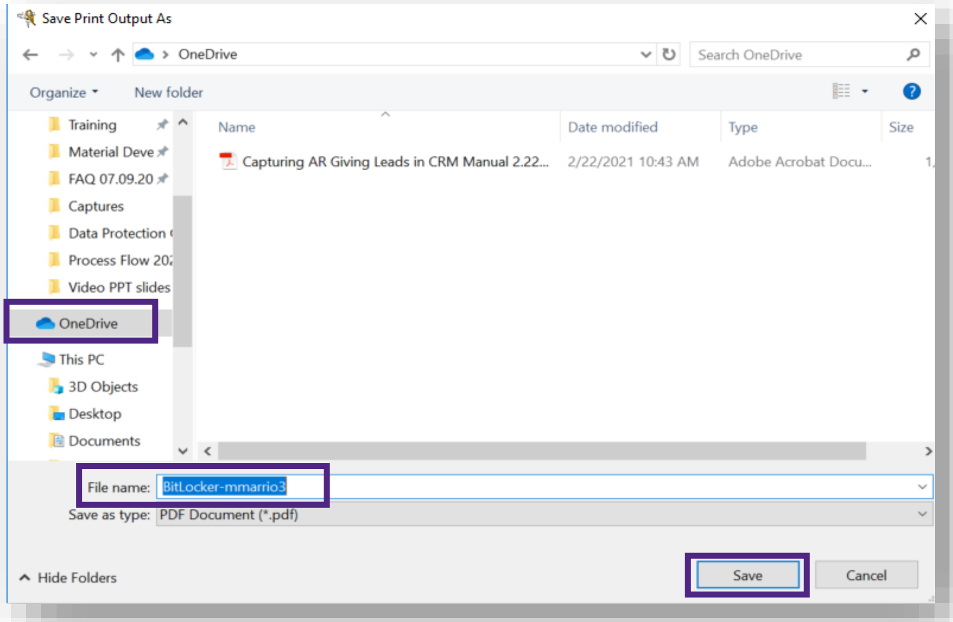
Location:

Comment:

● All

Number of copies: 1

- Save to OneDrive or W Drive as ‘BitLocker-username’ (E.g. BitLocker-mmarrio3)



Name	Date modified	Type	Size
Capturing AR Giving Leads in CRM Manual 2.22...	2/22/2021 10:43 AM	Adobe Acrobat Docu...	1,

File name: BitLocker-mmarrio3

Save as type: PDF Document (*.pdf)

- Click **Save**
- Click **Next**
- Click **Activate BitLocker**
- Send the file from OneDrive or the W Drive to your designated WTS support staff.

Windows Updates

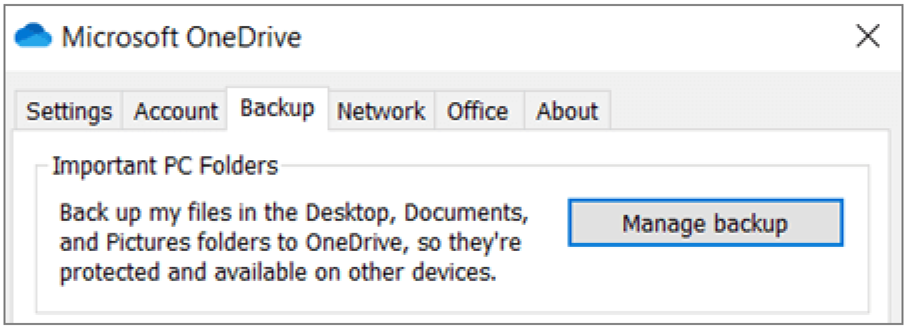
In Windows 10, Windows Update is found under Settings:

- Go to the **Start Menu**
- Click the **Gear/Settings icon** on the left
- Choose **Update & Security**
- Click **Windows Update** on the left
- Check for new Windows 10 updates by choosing **Check for Updates**

In Windows 10, downloading and installing updates is automatic and will happen immediately after checking or, with some updates, at a time when you're not using your computer.

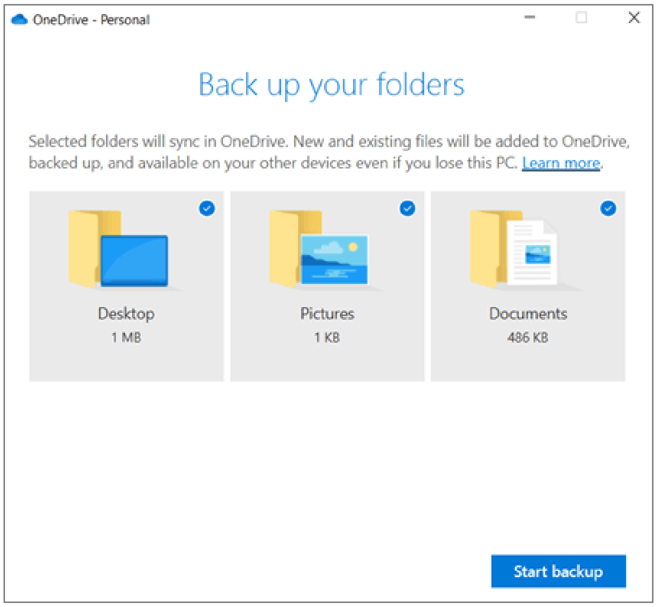
OneDrive Backup
Follow these steps to setup PC folder backup:

1. If you are prompted to back up your important folders (Desktop, Documents, and Pictures), select the prompt to start the folder backup wizard.
2. If you don't see a prompt or you have already closed the wizard, select the white or blue cloud icon in the Windows notification area, and then select **Help & Settings > Settings, then Backup > Manage backup**



Back up my files in the Desktop, Documents, and Pictures folders to OneDrive, so they're protected and available on other devices.

3. In the **Back up your folders** dialog, select the folders that you want to back up. Select **Start backup.**



Selected folders will sync in OneDrive. New and existing files will be added to OneDrive, backed up, and available on your other devices even if you lose this PC. Learn more.

4. You can close the dialog box while your files sync to OneDrive. Alternatively, to watch your files sync, select **View upload progress**. If you already closed the dialog, to open the OneDrive activity center, select the white or blue cloud in the notification area.