DATA SECURITY PACKET

Revised June 2015

About IronKey Devices

IronKey flash drives and hard drives are encrypted drives that are managed by Dental Informatics.

Differences between regular drives and IronKey drives

Hardware Encryption
Inside your device is the Imation Cryptochip, which protects your data to the same level as highly classified government information. This security technology is always on and cannot be disabled.

Password-Protected
To access your secure data, you unlock the device with a password using the Unlocker software that is carried on the device. Do not share your password with anyone. That way, even if your device is lost or stolen, no one else can access your data.

Self-Destruct Sequence
If the Cryptochip detects physical tampering by a hacker, or if the incorrect password is entered ten times, it initiates a permanent self-destruct sequence that securely erases all onboard data using flash-trash technology—**so remember your password**.

Set up the device

The setup process is the same for Windows and Mac systems.

1. Plug in the IronKey drive. The "Device Setup" screen appears. If the Unlocker window does not appear, you can start it manually by:
   - **WINDOWS**: Double-clicking the "IronKey Unlocker" drive in "My Computer" and launching "IronKey.exe".
   - **MAC**: Opening the IronKey Unlocker drive in Finder and opening the IronKey application in the IronKey Unlocker folder.
2. Type the Activation Code. You should have received the code in an email message sent from Imation Activation managed by Dental Informatics.
3. Select a default language preference, agree to the end-user license agreement, and then click the "Activate" button.
4. Type a device password and confirm it, and then click the "Continue" button.
   Your password is case-sensitive and must comply with the password policy listed on the right side of the password creation page.
5. A message prompt will appear indicating that an email has been sent to you. Follow the instructions in the email to set up your online account; this includes creating a "secret question".
6. Once you have set up your online account, click OK in the message prompt to proceed with the device setup.
7. The device initializes. During this process, it generates the AES encryption key, and creates the file system for the secure volume.
8. When the initialization is complete, the Imation Control Panel appears. Your device is now ready to protect your data and can be used on a Windows, Mac or Linux computer.

Unlock and lock the device

UNLOCK DEVICE

The unlock process is the same for Windows and Mac systems.

1. Plug in your device and wait for the Unlocker window to appear.
   If the Unlocker window does not appear, you can start it manually by:
   - *WINDOWS*: Double-clicking the "IronKey Unlocker" drive in "My Computer" and launching "IronKey.exe".
   - *MAC*: Opening the "IronKey Unlocker" drive in Finder and opening the IronKey application in the IronKey Unlocker folder.

2. Type your device password and click "Unlock." The Imation Control Panel will appear.
   - Entering your password correctly (which is verified in hardware) will mount your secure volume with all your secure applications and files.
   - Entering the wrong password 10 consecutive times will ***permanently destroy*** the device and all your onboard data.
   - As a security precaution, you must unplug and re-insert the device after every three failed password attempts.

NOTE: Contact Dental Informatics for assistance resetting your password.

LOCK DEVICE
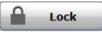
- Click the [🔒 Lock] "Lock" button in the bottom left of the Control Panel to safely lock your device.

NOTE: If you have applications or files open on the Secure Files drive, you might not be able to lock your device (this prevents potential file corruption). Close any open onboard applications and files and retry locking the device.

NOTE: An administrator can remotely lock your device, if necessary.

NOTE: Your device will automatically lock after 30 minutes if no files are being accessed.

CAUTION: Once the device is locked, you can safely unplug it. However, do not unplug the device when it is unlocked.

Access my device if I forget my password

If you forget your password, you can reset it by following the instructions below, or contacting Dental Informatics.

1. Plug-in your device and launch the Unlocker.
2. Click the "Password Help" button.
3. On the Password Help prompt, click the "Reset Password" button. An email will be sent to the email address provided during account setup with instructions on how to proceed.
4. After you complete the instructions in the email message, click the "Continue" button.
5. Type your new password and confirm the password in the fields provided, then click the "Change Password" button.

Change my password

It is good security practice to regularly change your password. However, be especially careful to remember your device password.

1. Unlock your device and click the "Settings" button in the menu bar
2. Click the "Password" button in the left sidebar.
3. Enter your current password in the field provided.
4. Enter your new password and confirm it in the fields provided.
5. Click the "Change Password" button.

Access my secure files

After unlocking the device, you can access the files securely stored on the device by:

- Clicking the "Files" button (folder icon) in menu bar of the Imation Control Panel.
- *WINDOWS*: Opening Windows Explorer to the "Secure Files" drive.
- *MAC*: Opening Finder to the "Secure Files" drive.

TIP: You can also access your files by right-clicking the IronKey icon on the Windows taskbar and clicking "Secure Files".

Encrypt and decrypt files

Everything you store on your Imation Enterprise device is encrypted. Since the device has a built-in Cryptochip, all of the encryption and decryption is done for you "on-the-fly," giving you the convenience of working as you normally would with a regular flash drive, while providing strong and "always-on" security.

- Drag a file onto the Secure Files drive to automatically encrypt it.
- Files opened from the Secure Files drive are automatically decrypted as you open them.

ENABLING BITLOCKER DRIVE ENCRYPTION ON WINDOWS 7

These instructions provide the procedure for turning on BitLocker Drive Encryption protection on an operating system drive of a computer with a TPM. After the drive is encrypted, the user logs on to the computer normally.

BitLocker Prerequisites

- You must be able to provide administrative credentials.
- You must be able to configure a printer if you want to print the recovery key.
- Your computer must meet BitLocker requirements (see below).

Enabling BitLocker for Windows 7

1. Click **Start**, click **Control Panel**, click **System and Security**, and then click **BitLocker Drive Encryption**.

2. Click **Turn On BitLocker** for the operating system drive. BitLocker will scan your computer to make sure that it meets the BitLocker system requirements. If your computer meets the requirements, BitLocker will inform you of the next steps that need to be taken to turn on BitLocker, such as drive preparation, turning on the TPM, and encrypting the drive.

If your TPM is not initialized, the BitLocker setup wizard will instruct you to remove any CDs, DVDs, or USB drives from the computer and restart the computer to begin the process of turning on the TPM. You will either be prompted to enable the TPM before the operating system boots or in some cases you will need to navigate to the BIOS options and enable the TPM manually. This behavior depends on the BIOS of the computer. After you confirm that you want the TPM enabled, the operating system will start and the **Initializing the TPM security hardware** progress indicator will be displayed.

If your computer does not have a TPM, you can still use BitLocker, but you will be using the **Startup key only** authentication method. All of the required encryption key information is stored on a USB flash drive, which the user must insert into the computer during startup. The key stored on the USB flash drive unlocks the computer. Using a TPM is recommended because it helps protect against attacks made against the computer's critical startup process. To use this method, your computer must support the reading of USB devices in the pre-boot environment and you must enable this authentication method by selecting the check box **Allow BitLocker without a compatible TPM** in the Group Policy setting **Require additional authentication at startup**, which is located in the following location in the Local Group Policy Editor: Computer Configuration Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives.

UNIVERSITY OF
LOUISVILLE.
SCHOOL OF DENTISTRY

3. After the TPM is initialized, the BitLocker setup wizard prompts you to choose how to store the recovery key. You can choose from the following options:

- **Save the recovery key to a USB flash drive**. Saves the recovery key to a USB flash drive.
- **Save the recovery key to a file**. Saves the recovery key to a network drive or other location.
- **Print the recovery key**. Prints the recovery key.

Use one or more of these options to preserve the recovery key. For each option that you select, follow the wizard steps to set the location for saving or printing the recovery key. When you have finished saving the recovery key, click **Next**.

Important
The recovery key is required if the encrypted drive is moved to another computer or changes are made to the system startup information. This recovery key is so important that it is recommended that you make additional copies of the key and store the key in safe places so that you can readily find the key if needed to recover access to the drive. You will need your recovery key to unlock the encrypted data on the drive if BitLocker enters a locked state. This recovery key is unique to this particular drive. You cannot use it to recover encrypted data from any other BitLocker-protected drive.
For maximum security, you should store recovery keys apart from the computer.

4. The BitLocker setup wizard asks if you are ready to encrypt the drive. Confirm that the **Run BitLocker system check box** is selected, and then click **Continue.**

5. Confirm that you want to restart the computer by clicking **Restart now.** The computer restarts, and BitLocker checks if the computer meets BitLocker requirements and is ready for encryption. If it is not, you will see an error message alerting you to the problem after you have logged on.

Warning
One of the items that BitLocker checks is the configuration of the system partition. BitLocker requires a minimum system partition size of 100 MB, and the Windows Recovery Environment requires 200 MB. When the operating system is installed, the system partition is automatically created by the setup process with a default size of 300 MB. However, this default partition size can be changed by computer manufacturers or system administrators when they install the operating system. If the system partition is exactly 100 MB, BitLocker setup assumes that you have a Windows Recovery DVD for use with your computer and the system check is completed without any errors. However, if you have a system partition size between 101 MB and 299 MB, the following error message will be displayed: "You will no longer be able to use Windows Recovery Environment unless it is manually enabled and moved to the system drive." If you have a Windows 7 DVD that contains the Windows Recovery Environment or you have another system recovery process in place, you may disregard this message and continue with BitLocker setup. Otherwise, you should check your system partition and verify that you have at least 200 MB of free space on your system partition so that the Windows Recovery Environment can be retained on the system drive along with the BitLocker Recovery Environment and other files that BitLocker requires to unlock the operating system drive.

6. If it is ready for encryption, the **Encrypting** status bar is displayed, which shows the progress of the drive encryption. You can monitor the ongoing completion status of the disk drive encryption by moving the mouse pointer over the BitLocker Drive Encryption icon in the notification area, at the far right of the taskbar. Encrypting the drive will take some time. You can use your computer during encryption, but performance might be slower. A completion message is displayed when encryption is finished.

By completing this procedure, you have encrypted the operating system drive and created a recovery key that is unique to this drive. The next time you log on, you will see no change. If the TPM ever changes or cannot be accessed, if there are changes to key system files, or if someone tries to start the computer from a disk to circumvent the operating system, the computer will switch to recovery mode and prevent Windows from starting.

WINDOWS COMPUTER SECURE USB/SD DEVICE ERASE

SDFormatter is installed on all Resident computers and on XenDesktop.

To securely erase SD cards follow instructions below.

1. Open SDFormatter
2. Select your Drive: Be sure to select the correct drive. Once erased data cannot be recovered.
3. Click "Option", change FORMAT TYPE to FULL (Erase), and click OK
4. Click "Format"

Note: This will securely format your device making all data unrecoverable and makes it writable.

1. Click on the **Applications** folder, then the **Utilities** folder and choose **Disk Utility**.
2. Select the USB/SD drive you want to erase from the list in the left panel.
3. Click the **Erase** category button on the top of the right panel.
4. Click the **Security Option** button.
5. Select "7-Pass Erase" for Secure Erase Options:
6. Click **OK** once selected.
7. Click **Erase**. Do not click "Erase Free Space" as this will not remove any data from the USB/SD device.
8. At the confirmation window, click **Erase** to start the erasure process.
9. A progress bar will appear in the lower right corner of the Disk Utility window with an estimated time for the erase process to complete. This may be several hours.
10. When erasure is finished, click the **Disk Utility** menu at the top, and choose **Quit Disk Utility**.
11. The USB/SD device should now be erased and ready for new use.

To set up FileVault, you must be an adminstrator. When you encrypt your information using FileVault, a recovery key is created as a safeguard. If you forget your login password, you can use the recovery key to unlock the encoded contents. The recovery key should not be physically stored with your Mac where it can be discovered.

WARNING: Don't forget your recovery key. If you turn on FileVault and then forget your login password and cannot reset it, and you also forget your recovery key, you won't be able to log in and your files and settings will be lost forever.

1. Choose Apple menu > System Preferences, click Security & Privacy, then click FileVault.
2. Click the lock icon 🔒 to unlock it, then enter an administrator name and password.
3. Click Turn On FileVault.
4. If your Mac has multiple users, a list of users appears. You can allow users to log in after the Mac starts up. If you don't, an administrator must log in before the user does.
5. For each user you want to enable, click Enable User, enter (or have the user enter) the user's login password, then click OK.
6. If the recovery key is hidden, click the triangle next to Show Recovery Key.
7. Copy the recovery key and store it in a safe place, then click Continue.
8. Choose whether you want the added safeguard of storing the recovery key with Apple.
9. Choose "Do not store the recovery key with Apple." and bring to recovery key to Dental Informatics for safe keeping.
10. Click Continue.
11. Click Restart.
12. After you restart, encryption begins. It may take some time to encrypt your information, depending on how much is stored. However you can use your Mac as usual while your information is being encrypted.

About iOS Encryption

Data protection is a feature available for devices that offer hardware encryption, including iPhone 3GS and later, all iPad models, and iPod touch (3rd generation and later). This article outlines how to enable and verify data protection.

iOS Products Affected

All Apple mobile devices to include iPad, iPod, iPod Touch, and iPhone.

Data protection enhances the built-in hardware encryption by protecting the hardware encryption keys with your passcode. This provides an additional layer of protection for your email messages and attachments

Enable data protection by configuring a passcode for your device:

1. Tap Settings > General > Passcode Lock.
2. Follow the prompts to create a passcode.
3. After the passcode is set, scroll down to the bottom of the screen and verify that the text "Data protection is enabled" is visible.

Passcode Tips

Use these passcode settings to maximize passcode security:

- Set Require Passcode to Immediately.
- Disable Simple Passcode to allow the use of longer, alphanumeric, passcodes.
- Enable Erase Data to automatically erase the device after ten failed passcode attempts.

If you misplace your iPhone, iPad, iPod touch, or Mac, the Find My iPhone app will let you use another iOS device to find it and protect your data. Simply install this free app on another iOS device, open it, and sign in with your Apple ID. Find My iPhone will help you locate your missing device on a map. You can then choose to display a message or play a sound, remotely lock your device, or erase your data on it.

To see all your devices in Find My iPhone, use the same *Apple ID* when you set up each device.

Set up an iOS device

1. On your device's Home screen, tap Settings, then tap iCloud.

   If you're asked to sign in, enter your *Apple ID*. If you don't have one, tap Create a new Apple ID, then follow the instructions.

2. If Find My iPhone (or Find My iPad or Find My iPod) is turned off, tap Find My iPhone, then tap to turn it on.

3. Tap to turn on Send Last Location.

   If your device is lost or stolen and its battery charge level becomes critically low, its location is sent to Apple automatically. When you use Find My iPhone to locate that device, you see where it was before its battery ran out of charge.

For added security, set up a passcode that needs to be entered before anyone can access the apps and information on your device. To set up a passcode, go to Settings > Passcode or Touch ID & Passcode. If your device has iOS 5 or iOS 6, go to Settings > General > Passcode Lock.

Set up a Mac

1. On your Mac, choose Apple menu > System Preferences, then click iCloud.

   If you're asked to sign in, enter your *Apple ID*. If you don't have one, click Create new Apple ID, then follow the instructions.

2. If Find My Mac is turned off, select it to turn it on.

   For added security, make sure your user account requires a password and that automatic login is turned off in Users & Groups preferences.

ENABLING DATA PROTECTION ON AN ANDROID DEVICE

Enabling Encryption for Android

Each manufacturer's menu layout may be different. Below we reference stock Android.
Note: You must have a **PIN** or **PASSWORD** lock screen enabled on your device before you can encrypt.

How to Configure Your Lock Screen

If you already have your lock screen configured, see "How to Enable Android Encryption":

1. Go to the **Settings menu** on your device
2. Scroll down "Security" or "Security and Screen Lock" or "Lock Scree"
3. Enter the "Lock Screen" menu and select "Screen Lock" under "Screen Security"
4. Select either **PIN** or **PASSWORD** and configure

How to Enable Android Encryption

Note: Make sure your phone is fully charged or plugged in before beginning this process. Encryption can take up to 30 minutes or more and if the phone runs out of battery, the process will fail and you will lose your data. Your phone will also reboot several times as it completes its encryption.

1. Go to the "Settings" menu on your device
2. Scroll down and select "Security"
3. Select "Encrypt Phone"
4. Complete the prompts and begin encryption!