BitLocker Setup

Part 1: For laptops and desktops WITH a TPM chip

Part2: For machines without a TPM chip (Optiplex 300 series)

Part 1

Enable the TPM Chip

- Boot into Setup (F2)
- Under the Security tab
    - Enable via "TPM Security", then choose "Save and Exit" and if "TPM Activation" is another option, immediately go back via F2 (D-series) and activate the chip.
    - (Some BIOS's have different settings – TPM Activation isn't an option – it's done as part of the second step below) (E-series)

Start BitLocker Encryption

- Login as an administrator (you must use a domain account, NOT pcadmin)
- Control Panel | BitLocker | Turn on the C: drive
    - Requirement check (~ 1 minute)
    - Prepare drive (3-6 minutes) then Restart when prompted
- If possible, have the user logon at this point (they must be an admin)
    - TPM initialization is automatically continued (2-3 minutes); some systems (E-series) require a restart and hitting the F10 key for TPM activation (it will prompt you)
    - The BitLocker window will automatically start but you need to hit "Next"
    - Print the recovery key (this should NOT be left with end-user and needs to be shredded after Frank/Alan verify that the Recovery Password is in the AD)
    - [Optional: Test the key before encryption – however the required reboot causes the encryption-GUI to not display progress – just click on the key icon by the clock, OR:]
    - Encrypt the drive – while this takes a long time, the users can do other things during the encryption – this is why you want to logon as them. The docs say you can shutdown and the encryption will restart on logon.

Notes:

- The entire disk is encrypted; files are unlocked when needed. Files copied onto the disk are encrypted, and files copied off are unencrypted. It's seamless to the end-user.
- If the hard drive is removed or mother-board replaced, the Recovery Key will be needed. Frank or Alan can get this to whoever needs it.
- Enabling the TPM chip can be done any time (part of imaging?) but BitLocker can only be done after the machine is on the domain

Part 2: BitLocker without a TPM Chip

Many desktops do not have a TPM chip (all the 300 series do not), but they can still be encrypted. You use a usb-key instead of the TPM chip. The key must be in the PC or it will not boot. The recovery key is still stored in AD.

- Login as an administrator (you must use a domain account, NOT pcadmin)
- Start | run | gpedit.msc
    - Go to: Computer Config | Admin Templates | Windows Components | BitLocker Drive Encryption | Operating System Drives
    - Double-click “Require Additional Authentication at Startup”
    - Select Enabled
    - Put a check in “Allow BitLocker without Compatable TPM”
    - Hit Apply and OK
    - “X” out of gpedit [the rest of this is the same as above]
- Control Panel | BitLocker | Turn on the C: drive
    - Requirement check (~ 1 minute)
    - Prepare drive (3-6 minutes) then Restart when prompted
- If possible, have the user logon at this point (they must be an admin)
    - TPM initialization is automatically continued (2-3 minutes); some systems (E-series) require a restart and hitting the F10 key for TPM activation (it will prompt you)
    - The BitLocker window will automatically start but you need to hit “Next”
    - Choose “Require a Startup key at every startup.”
    - Choose the correct removable drive and press save, then press “Next”
    - Print the recovery key (this should NOT be left with end-user and needs to be shredded after Frank/Alan verify that the Recovery Password is in the AD)
    - [Optional: Test the key before encryption – however the required reboot causes the encryption-GUI to not display progress – just click on the key icon by the clock, OR:]
    - Encrypt the drive – while this takes a long time, the users can do other things during the encryption – this is why you want to logon as them. You can shutdown – BitLocker will restart when the next user logs in.