eHealth Saskatchewan	**Name of Activity:** **Imaging/Re-Imaging Workstations** **Device Retirement / Clean Up**		
	Role Performing Activity: Deskside Operations		
WORK STANDARD	**Location: eHealth**	**Department: eHS CCS – Desktop Services**	
	Document Owner: **Danica Navarro**	**Region/Organization where this Work Standard originated:** **eHS CCS Physical Endpoint Management**	
	Date Prepared: **May 30, 2019**	**Last Revision:** **July 2, 2024**	**Date Approved:**

Work Standard Summary: This work standard will explain what is required to image a new machine or re-image an existing machine for re-distribution with the eHS Provincial Image.

Required BIOS Settings (Windows 10 and 11)

Confirm that the following settings are set in the BIOS:

- **UEFI is enabled and Legacy Boot is disabled**
- **The Integrated NIC is enabled with PXE Boot**
- **Secure Boot is enabled**
- **TPM is Enabled – (Version 2.0 required)**
- **SATA Operation is AHCI**

REQUIRED BIOS Settings (Windows 11 – New Builds)

- **When you access BIOS you will have READ ONLY access.**
- **You should see an "UNLOCK" button below a padlock Icon.**
- **In order to have access to EDIT the BIOS you will need to click "unlock" and type the password "B1OSd3ll"**
- **If you are Rebuilding a PC that has previously had the BIOS password set and booting from either PXE or USBBoot.iso on a USB key you will see the Prompt "Enter Admin Password, the [Enter}, to Continue. Type the BIOS password "B1OSd3ll" (you will not see a field to type this in but just key in the password on the keyboard) and then hit [Enter]. The boot process will continue normally from there**

Required BIOS Settings (Windows 7) Existing Windows 7 Machines only

Note: As of April 2024, there are still a few machines running Windows 7. Only existing Windows 7 machines are to be re-imaged with Windows 7

Confirm that the following settings are set in the BIOS:

- **Legacy Boot or UEFI is supported**
- **The Integrated NIC is enabled with PXE Boot**
- **Secure Boot is disabled – (Windows 7 does not support Secure Boot.)**
- **SATA Operation is AHCI**
- **TPM is enabled and version 1.2 – (Windows 7 only supports TPM version 1.2)**

Note: *For Dell System you can find the location of these setting in* ***Appendix A****. For other devices consult with the manufacture manual/website to determine how to set the system BIOS. This is also probably a good time to also check and update the BIOS version if it is not up to date. (See* ***Appendix B*** *for Updating Dell BIOS).*

Note: For TPM upgrade and downgrade instructions see **Appendix D.**

Prepping Workstation/Laptop for Redistribution

Before you can re-image a device you must perform the following steps, if this is a new device you can skip these steps, proceed to Imaging Workstation/Laptop

1. Run the Active Directory Users and Computers tool, connect to the domain the computer is currently joined to.

2. **Important:** Search for the machine that you are about re-image and delete the computer object. This ensures that the machine isn't assigned to any groups or OUs that aren't required after the rebuild.

3. Login in to the SCCM Console, click on Devices and search for the system you removed from the previous step.

4. Once the computer object is displayed in the results, right click on the object and choose Delete, confirm the deletion of the device. Once the device is removed continue with the imaging process. If the device or MAC address is not removed from SCCM you will not be able to image the device.

   Note: For Shared Docking Stations/USB Ethernet Dongles used for Imaging:
   - MAC Addresses need to be omitted in SCCM
   - You will notice devices will fail to PXE boot or USB boot will show no task sequences are available.
   - Please log a ticket to the eHS SCCM Services Group with the MAC address of the shared dock or dongle.

   Note: If you don't have permissions to access a domain and/or the SCCM Administration Console, please submit a Ticket to the eHS Service Desk to have the device deleted.

Imaging Workstation/Laptop

1. Prior to Imaging, confirm that the BIOS is configured with the settings mentioned above and the device is connected to the network through an Ethernet cable. Select the best option under **Appendix C** to image the device. If you are unsure on which option to use, consult with the eHS CCS – Physical Endpoint team.

2. At the DELL logo screen, press F12 to access the one-time boot menu, select the appropriate boot device (USB or NIC IPv4) based on your selection from **Appendix C**. If prompted press enter to continue the boot process.

   Note: *You may have to consult with the devices manual on how to invoke the "One Time Boot" option. If you have a local distribution point you may need to use the USB boot option under* ***Appendix C*** *if PXE is restricted on your network. Consult with your network administrator or the provincial SCCM team if you are unsure which method to use.*

3. Once you see the **"Welcome to the Task Sequence Wizard"** you'll be asked to enter a password, the password is **"1magem3"** without quotes then click next.

4. You should now be asked to choose the Task Sequence you would like to Run:

   - **Prod | Win 11 – M365 Apps** *(Only to be used for Organizations with Win 11)*
   - **Prod | Win 10 – M365 Apps**
   - **Prod | Win 10 – Office 2016**
   - **Prod | Win 10 – Kiosk**
   - **EOL | Windows 7 Enterprise – Office x86 (Only to be used for existing Windows 7 machines)**

   Select the task that best suits your environment. If you see images label DEV/UAT or VDI please do not use them for production purposes. If no task sequences are available for the machine, verify the object was removed from SCCM, refer to the Prepping Workstation section.

5. After your selection the wizard should take to the "Microsoft Deployment Toolkit Wizard", click Next.

6. In the “Deployment Readiness Screen”, confirm that you have a green check mark beside each listed item then click Next. If you get an “X” beside one of these items, see about correcting the issue and press Retry Check, if everything passes click Next.

7. Under “New Computer Details” enter the Machine Name (following the Naming Standards) you are assigning to this device and select the Domain you want this machine to be added too, select the appropriate OU if multiple are available and click Next. If joining to the SKHealth domain select the appropriate area OU (“eHealth” or “SHA”).
   Note: Expand to the proper sub-OU for SHA in SKHEALTH

8. Confirm that the Time Zone for the machine is set correctly and click Next.

9. Review the Summary, if everything is correct click Finish and the wizard will start loading the selected image on the machine.

10. If there aren’t errors or issues loading the Image to the device, you should eventually see a “Deployment Complete” Window and a button that says “Start Windows.” Once you’re at the Windows login page, the process is complete.

    Note: If you experience errors during the imaging process, examine the c:\windows\ccm\logs\smsts.log for errors. Also verify the boot option selected is UEFI based and not legacy if multiple options are available. If you are unsure of the error please log a ticket to the eHS CCS Physical Endpoint team and attach the log for further assistance.

11. Verify the bitlocker recovery key is available.

Device Retirement / Clean Up

If a device is replaced or retired, please follow the device retirement/clean up process below.

1. Run the Active Directory Users and Computers tool, connect to the domain the computer is currently joined to.

2. **Important:** Search for the machine that you are about re-image and delete the computer object. This ensures that the machine isn’t assigned to any groups or OUs that aren’t required after the rebuild.

3. Login in to the SCCM Console, click on Devices and search for the system you removed from the previous step.

4. Once the computer object is displayed in the results, right click on the object and choose Delete, confirm the deletion of the device. Once the device is removed continue with the imaging process. If the device or MAC address is not removed from SCCM you will not be able to image the device.

Appendix A – BIOS Configuration setting for Dell Devices

This where you can find the required BIOS settings that are need to be set prior to Imaging a Windows 10 device.

- **Enabling UEFI Boot Sequence**

  Boot Sequence -> Click the button for UEFI

- **Disable Legacy Boot**

  Advanced Boot Options -> Un-Check “Enable Legacy Option ROMs”

- **Enable NIC with PXE boot**

  System Configuration -> Integrated NIC ->

Place a Check box beside “Enable UEFI Network Stack”
Click the button beside “Enable w/PXE”

- **SATA Operation**

  System Configuration ->SATA Operation -> Click the Button for AHCI

- **Enable TPM**

  Security -> TPM 2.0 Security -> Place a Check beside “TPM On” and Click the button for enable.

- **Enable Secure Boot**

  Secure Boot -> Secure Boot Enable -> Click the button for enable

Appendix B – Updating BIOS on Dell Systems

The follow instructions are from Dell, you’ll need to download the latest update from Dell support prior to these steps.

Updating the BIOS from Windows

Note 1: Before updating the BIOS, ensure that you suspend BitLocker encryption on a BitLocker-enabled system. If BitLocker is not enabled on your system, you can ignore this step.
Note 2: Do not turn off the power or interrupt the BIOS update process during the update.

Download and Installation
1. Click Download File, to download the file.
2. Click Save to save the file to your hard drive.
3. Browse to the location where you downloaded the file and double-click the new file.
The system restarts automatically and updates the BIOS at the system startup screen. After the BIOS update is complete, system restarts again.

Updating the BIOS from BIOS Boot Menu (independent of operating system)

Note 1: Before updating the BIOS, ensure that you suspend BitLocker encryption on a BitLocker-enabled system. If BitLocker is not enabled on your system, you can ignore this step.
Note 2: Do not turn off the power or interrupt the BIOS update process during the update.

Installation
1. Copy the downloaded file to a USB drive. The USB drive does not need to be bootable device.
2. Insert the USB drive into any USB port.
3. Power on the system.
4. At the DELL logo screen, press F12 to access the one-time boot menu.
5. Select BIOS Flash Update in the Other Options section.
6. Click the ... button to browse the USB drive to locate the downloaded file.
7. Select the file and click Ok.
8. Verify the existing system BIOS information and the BIOS update information.
9. Click Begin Flash Update.
10. Review the Warning message and click Yes to proceed with the update.
The system restarts and displays a progress bar at the Dell logo screen. The system restarts again when the update is complete.

Appendix C – Options for loading an SHA Image to a Device

PXE Boot

This allows you to boot and image a device over the network where a local distribution point is available. Consult with your local team or the provincial SCCM team if this option is available on your network.

USB Online Boot

This allows you to boot via USB and image a device over the network where a local distribution point is available. Select this option if PXE Boot isn't allowed or is not supported by the device. You'll require a 500MB flash drive or greater.

1. Format the USB drive to FAT32
2. Copy the **USBBoot.iso** from \\cs-n-1037.skhealth.ca\images\
3. Extract the content of ISO to the root of the flash drive. (This can be done by Mounting the ISO and Coping the contents from the Mounted ISO to the USB Drive or install 7-Zip from the Software Center and using 7-ZIP to Extract the ISO contents to the USB Drive)
4. Once the boot drive is created, Boot the device from this USB Drive and run through Steps 2-9 in the Imaging Process.

USB Offline Boot

This allows you to boot and image a device via USB where a local distribution point is not available. You will require at least a 32GB flash drive.

These images expire on a periodic basis to ensure you are using an up to date version. If you encounter an expiration error you will need to re-download the offline. Check the ReadMe-Windows10.txt in the same share for details.

1. Format the USB drive to FAT32
2. Copy the appropriate **WinxOfficexOffline.iso** from \\cs-n-1037.skhealth.ca\images\
3. Extract the content of ISO to the root of the flash drive. (This can be done by Mounting the ISO and Coping the contents from the Mounted ISO to the USB Drive or install 7-Zip from the Software Center and using 7-ZIP to Extract the ISO contents to the USB Drive)
4. Once the boot drive is created, Boot the device from this USB Drive and run through Steps 2-9 in the Imaging Process.

Note: The offline image does not contain all the available drivers due to space restrictions. Consult the ReadMe-Windows10.txt in the same share for details and updates. To inquire about updating or adding drivers please contact the Provincial SCCM team.

Appendix D – Updating or downgrading a TPM device

Dell Systems

For instructions to upgrade or downgrade the TPM firmware on Dell systems refer to the following link:
https://www.dell.com/support/article/us/en/04/sln300914/trusted-platform-module-tpm-upgrade-downgrade-process-for-windows-7-and-10-operating-system-upgrade-downgrade?lang=en

HP Systems

For instructions to upgrade or downgrade the TPM firmware on HP systems refer to the following link:
https://support.hp.com/ca-en/document/c05381064