Mac Imaging Documentation

Overview: This documentation will walk you through the Mac imaging process.

Requirements: USB imaging key, power cord, ethernet connection.

Steps:

Step 1) Connect power and ethernet to MacBook and insert USB key.

Step 2) Restart the Mac and hold CMD+R while rebooting, until the Apple logo with a white loading bar appears.

Step 3) When booted in, select “TechZone loaner” as the user, and enter the TZ password.

Step 4) Select disk utility

Step 5) Select the primary disk volume (Usually labeled as Macintosh HD and/or Data.

Step 6) Select “erase”.

Step 7) Once these partitions are erased, delete any sub-volumes (such as those labeled “data”).

Step 8) Reboot the Mac and hold the option key.

Step 9) Select “Install MacOS X” from the boot key option.

Step 10) Follow install prompts and select “Macintosh HD” as the primary installation disk.

Step 11) Installation will now begin. Once MacOS has finished installing, proceed to step 12.

Step 12) Select language- English, and country- US.

Step 13) Make sure you see the “Remote Management” setup page, and press continue.

Step 14) Set username as precat, with the Wildcat password.

Step 15) Enable location services. You will then be signed into the device.

Step 16) Wait for self service to pop up, then follow the prompts. This will download Villanova software and will take ~20 minutes.

Step 17) Create a new user. Do this by going to System preferences> Users and Groups> Add account

Step 18) Set the user as Administrator and name the account techzone (with no caps).

Step 19) Set the account with the TZ password.

Step 20) Exit settings and restart device.

Step 21) Sign in with the TZ account, and open terminal.

Step 22) Run the following commands through terminal:

```
Sudo jamf recon

Sudo jamf policy
```

Step 22) Navigate back to users and groups and delete the Precat account with its home folder.

Step 22) Re-run the sudo commands listed in step 22. This will prompt a reboot script.

Step 23) After the reboot, sign in to techzone and open terminal, then run the above commands again. To check for encryption, run one last command:

```
Sudo fdesetup status
```

Step 3) If file vault is enabled, then device is encrypted and ready to be placed back on shelf.