Installing Whole Disk Encryption – Best Practice

1. Check for any pending Microsoft Updates with the “Microsoft Update” utility. Reboot the machine if needed to install any updates that are found. (Refer to How to Check for Windows Updates document)
2. Make sure that an older encryption client is not installed. This can be found in “Programs and Features” in the control panel. Look for software titled Guardian Edge or Symantec Endpoint Encryption. (Refer to How to Check your Computer for older version of Encryption)
3. Be sure Bitlocker is not enabled – Control panel > Bitlocker Drive Encryption – this will tell the status of the drive. If it is on, do not proceed.
4. Run Disk cleanup, check all boxes with the exception of “Catalog files for the content indexer” (Refer to How to Run Disk Cleanup)
5. Back up user files “C:\Users\Username” (Refer to How to Backup your User Profile)
6. Perform a disk defragment (Refer to How to do a Disk Defragment)
7. Run chkdsk to be sure the drive is healthy (How to Run Check Disk)
8. Install encryption (Refer to Symantec Encryption Desktop Install Instructions)

Each Department must enter all their computer devices into the WASP Inventory application. This can be done before or after the encryption is complete. However, once the encryption is complete you will have to go to WASP and ensure that the Encryption field is updated. (Refer to WASP – How to Add an Asset)