**Encryption Best Practices Guide For Windows 7 Laptops**

**Background:** Because laptops are capable of maintaining power after being unplugged it is important to note that the data on them is only fully protected by encryption when the machine is powered off or in hibernation mode. That is why it is also important to ensure that the power saving settings on laptops are modified to ensure that the data is hibernated when not in use for extended periods of time.

Once the Symantec PGP encryption client is installed on your laptop it is recommended that you modify the default power settings. This document contains instructions for setting your laptop up in hibernation mode. These changes will ensure that when it’s left unattended for long periods of time, and when the lid is closed, the data will be securely encrypted. This is particularly important to consider when traveling with a machine that contains sensitive data.

**Windows 7:**

**Hibernation Settings**

Many of the settings mentioned here are found in the menu list as shown below (Control Panel / Power Options / Choose what the power buttons do):



Under the option to “Choose what the power buttons do and validate your settings” (as seen below). It is recommended that you choose either “Power off or Hibernate” for all of the options listed here and click “Save changes”.



Click the “Change advanced power settings”



Set the “hibernate after” to a set time that you feel comfortable with and click the “OK” button. If you forget to lock your screen when you walk away, this setting it will ensure that your computer automatically goes into hibernation mode after for example 20 minutes of inactivity.



**Help:**

Please work with your departments Tier I support for assistance and or questions regarding any of the items listed here. Otherwise you can contact the IT HelpDesk at 852-7997 or helpdesk@louisville.edu.