1. Are all Business Units required to purchase encryption licenses?

   A. The Office of Information Technology has implemented a disk encryption policy that applies to all Emory-owned, and personally-owned, desktop and portable computing devices storing Emory-managed data as defined by Emory Policies and Procedures Policy 5.12 Disk Encryption Policy.

2. What time frame is needed for funding? Can we buy licenses as needed or do we have to fund all of the licenses at once?

   A. The time frame, as defined in Policy 5.12 Disk Encryption Policy, is effective immediately for new systems. Existing systems have 6 months from the effective date of this policy to fully implement the requirements, unless otherwise noted.

   The seats can be purchased as needed in groups of 10 or greater. (unless total purchase is less than 10)

3. Is this licensing a onetime or a yearly license fee?

   A. The licensing is a onetime fee. Current pricing is $45.50 per seat.

4. Can licenses be funded from research/program grants?

   A. The cost model should meet with service-center requirements, in that we are not making a profit or a loss on the recharge. The grant owners should consider the purchase as “software.” As long as software is an eligible commodity on the grant, there should be no problem from our side. The costs are real and auditable. Not all grants allow software purchases, but many do. The grant owners should know whether their grants are eligible.

5. How are licenses purchased?

   A. To purchase licenses: submit a request via email to OIT Finance & Administration -John Connerat (jconner@emory.edu), Carole Hirthler (carole.hirthler@emory.edu) and Sandra Harrison (sharr06@emory.edu) with the following information:

   - division/dept name
   - contact name/info
   - number of licenses (requested in groups of ten or greater)
   - SmartKey

   Once the charges are applied to your account, the OIT Information Security Group will activate the licenses and contact your Local IT/Desktop support with installation information.
Emory Disk Encryption Policy
PGP Whole Disk Encryption
Frequently Asked Questions

6. What is the end-user experience?

A. The only change in the end-user experience with PGP Whole Disk Encryption is the addition of a pre-boot authentication screen and password changes. The pre-boot authentication screen protects the system from being accessed by unauthorized users by disabling their ability to attack operating system–level authentication mechanisms. Once the end user provides valid authentication, encryption and decryption of the disk are transparent to both the user and the operating system. The pre-boot authentication passphrase can be synchronized with the Windows logon, enabling Windows users to be automatically logged into their system without requiring additional passphrases or user actions.

7. What performance impact should be expected when PGP Whole Disk Encryption is in use?

A. Once the hard drive is encrypted, the performance impact of PGP Whole Disk Encryption is negligible. Some users may notice a performance impact during the initial encryption process; however, this is a one-time-only event during which all current-generation PCs will perform normally, although disk-intensive computing processes may take slightly longer. The initial encryption process can be suspended at any time to complete time-sensitive or disk-intensive tasks.

8. Does PGP encrypt Flash Drives (portable devices)?

A. Yes. You must be enrolled in a PGP policy that enables you to manage removable media encryption. PGP must be installed on any system that you wish to use to access the flash drive.

9. Is there additional information, Q & A or technical discussion to understand how the encryption licensing works?

A. There have been presentations and discussions at monthly IT Briefings over the past year. There will be a PGP Disk Encryption review on the January 21, 2010 IT Briefing agenda. Detailed technical information will be provided in the IT and Desktop Support training sessions in addition to a new Information Security - PGP Service webpage.