Emory PGP deployment prep steps

There are six pieces to preparing for PGP deployment at Emory:

1. Licenses
2. Groups
3. Policies
4. Training
5. Software
6. Server access (optional)

Licenses
Ensure licenses are purchased to cover all computers running PGP Whole Disk Encryption (WDE). Our PGP WDE arrangement is for perpetual PGP WDE licenses at $45.50 per seat, so a license is required for each computer running the PGP software.

Licenses may be purchased by sending a Remedy ticket or an email to securityteam-l@listserv.emory.edu containing the following information:
- School/Division/Business Unit name.
- Requestor’s contact information.
- Number of licenses being purchased.
- Smart Key number.

Groups and Policies
The PGP WDE software allows for policy-based configuration that is keyed off of Active Directory group membership. By default, each department will have two policies – one for regular users and one for IT staff who need full access to PGP functions. These policies can be customized if needed. To associate users with the correct policies, you’ll need groups in either the Emory University Active Directory (Emoryunivad) or Emory Healthcare Active Directory (euhcs). You can create new groups, or use existing groups. The groups associate users to policies and then the policies determine how PGP works while that user is logged in.

Training
The OIT Information Security office will provide either group or one-on-one training on the PGP software and the PGP policy configuration options. Contact the office using Remedy or email securityteam-l@listserv.emory.edu

Software
After policies are set up, the security team will send you information on downloading the installer for the PGP software. Installers are available for Windows 32-bit, Windows 64-bit and OS X on Intel CPUs.
**PGP server access**
Each department may have one or two IT staff with access to log into the PGP Universal Server to retrieve Whole Disk Recovery Tokens (WDRT) in the event that a user forgets their password. The University and Healthcare IT service desks also have this ability, so this is an optional item.

**Steps to deploy recap**

1. Get licenses
2. Create AD groups (or identify existing ones)
3. Contact information security about PGP training
4. Request department PGP policies using Remedy or email securityteam-l@listserv.emory.edu, including the following information
   a. Department name
   b. Department IT contact
   c. AD groups and which policy to associate them with (user or admin)
   d. NetID of the user who needs access to download the software
5. Download software
6. Get PGP server access (optional)

**Software testing and deployment**
Each group can use their existing software deployment processes to install the PGP software onto computers, but departments should first test the software extensively. Prior to deploying the software to systems, a disk media check (“chdsk /r” for Windows) should be run on the computer. **Be sure to backup any important data before beginning a disk encryption process.** PGP can be deployed using any desktop management system that supports the distribution of MSI installers for Windows, or .pkg installers for Mac. Examples include LANDesk, Absolute Manage, and Microsoft SMS.

**Note:** Do not deploy PGP as part of your standard build image for new systems. **PGP should only be installed on systems to comply with Emory’s Disk Encryption Policy (http://policies.emory.edu/5.12), or on an as needed basis.** Also, local IT support personnel should never use their own credentials to enroll an end user’s system with PGP. **The end user should use their own NetID and passwords to enroll when they first log in to a new system, or their existing system after PGP has been installed.**