

PGP WDE Service Notes

General Information about PGP

The recommended implementation of PGP WDE at Penn requires connecting your computer to a PGP Universal Server. Please work with your local support provider to obtain the software and assistance necessary to access the appropriate PGP server for your school or center.

Using a computer that is encrypted with PGP Whole Disk Encryption raises some important issues that users need to consider:

- **Back up your computer regularly.** Although backing up your computer is always the best practice, the addition of encryption makes it even more important to regularly make a back up copy of your data. On an encrypted hard drive, data that is lost due to hard drive failure or human error will not be able to be recovered by standard data recovery tools and services.
- **Have a strong system password.** Your PGP password will be required when first starting up your computer; however, it is still very important to have an additional strong system password set on your laptop or desktop in order to fully protect your data. For example, if your laptop goes to sleep, only the system password will be required to wake it up—the PGP password will not be needed.
- **Token Recovery.** Through a managed Universal Server, Penn will have the ability to generate a recovery token, which can be used to reset your PGP passphrase. In the event the local password is lost, it will still be possible to access the data on your encrypted computer using this recovery mechanism.
- **Export Controls.** Users intending to travel to Cuba, Libya, North Korea, Syria, Sudan, Iran or Iraq must contact the Office of Research Services for assistance in determining whether an export license is required, and, if so, assistance in applying for an export license (see <http://www.upenn.edu/researchservices/exportcontrols.html> and <http://www.bis.doc.gov/policiesandregulations/regionalconsiderations.htm>). In addition, any release of the technology or source code to a foreign national from Cuba, Libya, North Korea, Syria, Sudan, Iran or Iraq, or an individual on the denied parties list (see <http://www.bis.doc.gov/dpl/thedeniallist.asp>), even while in the United States, may be prohibited under the “deemed export” rules. Again, you are responsible for contacting Penn’s Office of Research Services for assistance.
- **Other PGP Restrictions.** PGP products may not be used directly or indirectly in the design, development, fabrication, or use of nuclear, chemical, or biological weapons or missile technology without US government authorization. Contact the Office of Research Service for more information.

Security check points in travel

If feasible, faculty and staff may wish to take an alternate, “clean” computer when traveling to avoid exposing sensitive data to inspection staff.

- Beyond export laws, please be aware that certain countries have been known for inspecting laptops and data upon entry, so you should be extremely careful about any proprietary, patentable or sensitive information that may be stored on your device. PGP has informed Penn that Russia and the People’s Republic of China may currently restrict the importation of PGP’s encryption software, including bringing a laptop with the software installed into those countries.
- US Homeland Security may also decide to inspect your laptop when you return to the US, and by law they have the right to inspect.