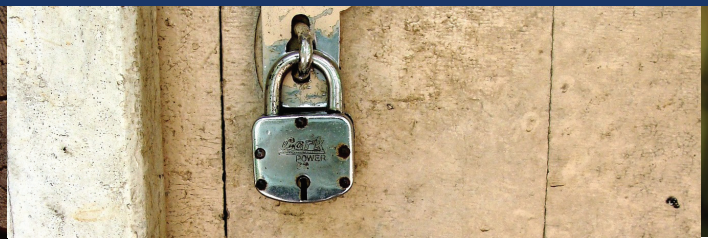




In May 2014, President John Fry announced the expansion of the Data Security Initiative, a component of the University's comprehensive security, privacy, and compliance program. This initiativeis aimed at protecting academic, medical, financial, and other sensitive personal records entrusted to the University, providing peace of mind to students, patients, faculty, and professional staff. All IT groups at Drexel are working to ensure that University-owned computers are protected by December 2014.

## Computer Encryption

University-owned hard drives will be encrypted with Sophos SafeGuard. Faculty and professional staff whose computers are not already protected will be contacted by an IT professional to begin the process:

### *Assessment and Preparation*

An IT consultant will make an appointment to visit your office to make a backup of your files using CrashPlan Pro Enterprise. If your department head has subscribed the CrashPlan backup service for you, the software will provide continuous backup from that point on; if not, the software and temporary backup will be removed from your computer after encryption.

Once the initial backup is complete, the consultant will return to ensure that your computer has supported, updated versions of Windows or Mac OS X. If your computer has an "uncommon" setup, the consultant will present options for a standard setup that will allow encryption.

Finally, the drives in your computer will be checked for integrity. Typically, this process runs overnight.


### *Computer Backup*

If you choose to continuously back up your data, Drexel has selected CrashPlan Pro Enterprise as its backup solution for Windows and Mac OS X. CrashPlan provides unlimited storage for up to four computers per user and meets Drexel's current security requirements. To request CrashPlan service, contact IRT Accounts at **accounts@drexel.edu**.

### *Installation and Restart*

Once the integrity of your drive is confirmed, Sophos SafeGuard Enterprise will be installed. Installation typically takes 15-30 minutes. A small number of computers will require additional technical support.

### *Initial Encryption*

After the installation and restart, you will sign in to your computer and the initial encryption will begin. The time needed for initial encryption depends on the capacity and speed of the storage drives, but on average requires a few hours. Normal performance resumes after completion.

## Unsuitable Backup Methods

USB hard drives and flash memory drives should not be used for primary backup. They are not encrypted to Drexel standards and thus negate the protection encryption provides.

If secure, portable storage is needed, you may purchase one of these products recommended by the College of Medicine at: **http://it.drexelmed.edu/LaptopEncryption.aspx**.

IRT-provided file servers may not be used for computer backup purposes. Similar restrictions may apply for file servers operated by other departments.

## File Server Encryption

Groups that need to share files that contain highly sensitive Personal Health Information (PHI) or Personally Identifiable Information (PII) such as Social Security numbers, driver's license numbers, banking account numbers, etc., must store the information encrypted on a file server meant for this purpose.If your group needs encrypted files server space, please send an email to **infosec-request@drexel.edu**.

## Protecting Smartphones and Tablets

Current security measures call for a 6-digit PIN. Since most mobile users already have a 4-digit PIN, they'll be asked to choose a longer one when they access Drexel email for the first time on their device. These security measures also require that the screen turn off within 15 minutes and prompt for the PIN again if more than 15 minutes have elapsed since last use.

Next, your device will be instructed to encrypt. Some older devices can't encrypt and will stop receiving email when the new security policy is implemented. If this happens, contact IRT at 215-895-2020 (**consult@drexel.edu**). IRT is permitted to provide temporary accommodation for such devices through December 31, 2014, after which such devices will need to be replaced to continue receiving Drexel email.

Most importantly, these security measures instruct the device to erase itself if the PIN is mis-entered 15 times in a row. (Your mail, calendar, and contacts are safely stored on the server, but photos and other data could be lost if not backed up elsewhere.) Be careful when entering your PIN and never share it with others.

## Email Data Loss Protection

IRT scans outbound messages for sensitive information. The definition of "sensitive" will change as the system is continually reconfigured to protect data required by law or common sense.

Messages sent from an IRT-managed email system to another email system ("outbound") with sensitive content will be blocked if they exceed a security threshold. The email system will provide you with an explanation of what kind of information was found and provide instructions for

attempting redelivery.

If the sensitive content warning was unexpected, you should review the message, its attachments, and the recipient addresses. You might have inadvertently attached a file (or the wrong file) or mistyped an address.

Sensitive information should be removed if it is not needed. Remember to check for hidden content such as spreadsheet rows and columns or presentation slides that aren't showing. Sometimes, charts and tables in word processing documents embed difficult-to-locate source data that contain more information than necessary.

If you removed content as a result of a review, you may try sending the message again. It will be rescanned and delivered if it no longer contains sensitive information. If the sensitive information is essential for the message, it can be encrypted and sent by adding the phrase **[reviewed-resend]** (invisible to recipients) to the subject line.

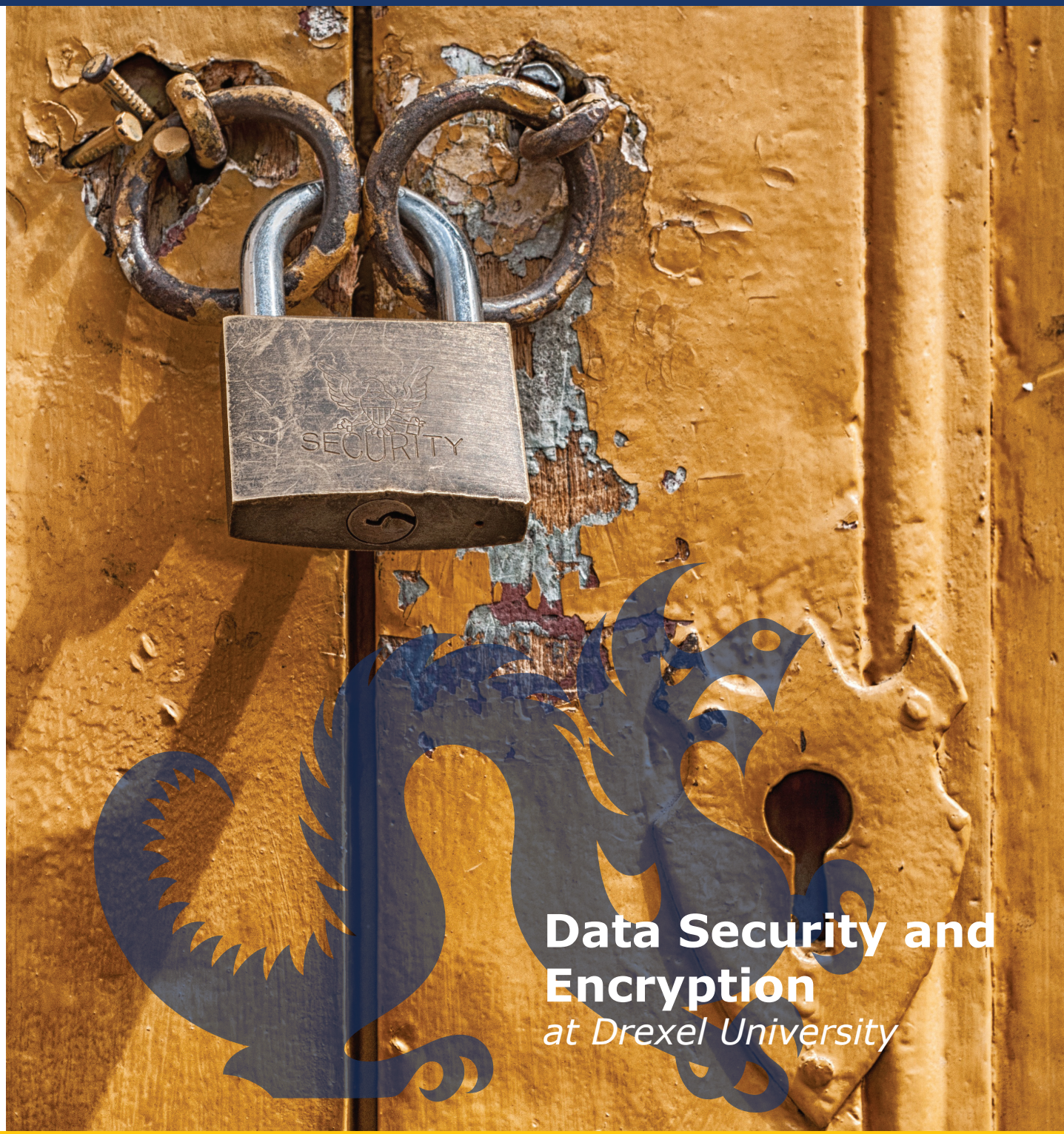
### *Encrypted Other Messages*

You may also encrypt other messages if you want to ensure safe delivery. To do so, add **[encrypt]** (also invisible to recipients) to the subject line before sending it.

### *Receiving Encrypted Email*

When someone outside of Drexel receives an encrypted message for the first time, they will be invited to set up an encryption account. Afterwards, encrypted messages will be delivered as password-protected PDF files. The PDF includes a "Reply" button to encrypt replies; using Outlook's "Reply" button will not encrypt, but it also will not include the sensitive data, keeping the communications secure.


**Korman Computing Center**
Office of Information Resources and Technology
33rd Street (between Market and Chestnut St.)
215-895-2020 or consult@drexel.edu
www.drexel.edu/irt


# Data Security and Encryption

*at Drexel University*