



BSD Information Security



August 2015
Volume 1, Issue 8

Encryption Awareness Month

In this issue of the BSD ISO Cybersecurity Newsletter...

- **September 2015 is Encryption Awareness Month** – The BSD ISO is declaring September Encryption Awareness Month! Please see the enclosed information on how you can encrypt your devices to enable the secure transmission of data and protect your information. (*Page 1-2*)
- **Encryption Posting Poster Contest** – Spread the word about encryption by posting the BSD Encryption Poster throughout your workspace and **win a \$250 Amazon Gift Card**. (*Page 3*)

September is Encryption Awareness Month



What is Encryption?

- Uses a mathematical function to scramble data
- Prevents access to data from unauthorized parties



Why should you Encrypt?

- Electronic devices are lost and stolen daily from home, car and work
- Information stored on these devices can be used to:
 - Steal your identity
 - Tarnish the University's reputation
 - Sold to others online



What should you Encrypt?

- Laptop
- Email
- Mobile devices
- USB flash drives



When should you Encrypt?

- Using your device for work related activities
- Emailing sensitive information (e.g. PHI, PII, SSN etc.)
- No one else but you or those that you trust should see

Dance like nobody's watching...Encrypt like everybody is!

The following table provides general information on how to encrypt devices and information. For specific information about encryption options visit our encryption website <http://security.bsd.uchicago.edu/encryption>.

If you have a Laptop...

The BSD ISO's Encryption Self Service Portals assist BSD employees with encrypting Apple and Windows laptops.



Encrypt using the BSD Self Service encryption solution for Apple laptops.
Use this link to access the Self-Service portal: <https://encryption.cri.uchicago.edu/enroll/>.



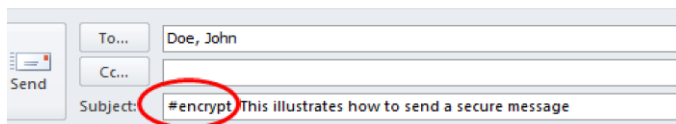
Windows

Encrypt using the BSD Self Service encryption solution for Windows laptops.
Use this link to <http://security.bsd.uchicago.edu/encryptwindows/> to download and install.

If you need to send a secure E-mail...

The enterprise Secure Email Portal is available to the entire BSD community. The Secure Email Portal allows for the automatic encryption of email messages sent outside of the BSD.

How to Send a Secure Email - To send a secure email, just add **#encrypt** (both hash mark and the word "encrypt") to the subject line of your e-mail. This will trigger the email system to send the email with encryption over the Internet.



How Your Recipients Retrieve Your Secure Message - Correspondent will be provided a link to log in to the Secure Email Portal to retrieve the message. The first time your recipient receives a secure email, they will be asked to create a password. The same password would be used to review any subsequent secure email messages they receive.

If you have a Mobile Device...

The following are safeguards you can use to reduce the risk of someone accessing personal and organizational data when your mobile device is lost or stolen.



iOS version 4.0 or higher with a passcode set will automatically be encrypted.

To set the passcode:

Go to Settings > General > Passcode. Follow the prompts to create a passcode.



Android

Android version 4.4 or above can be encrypted with a built in "Encrypt your phone" functionality.

To encrypt:

Set a lock screen PIN, pattern, or password. Open the Settings menu on your device.

Under "Personal," touch **Security**. Under "Encryption," touch **Encrypt tablet** or **Encrypt phone**.

If you use USB flash drives...

Several manufacturers provide encrypted USB drives. The following models are approved for use and provide strong encryption.



Aegis

Aegis USB - Uses strong hardware-based encryption. Compatible with any operating system. Finger leave no telltale trace on tough PIN pad keys www.apricorn.com/aegis-secure-key.html.

Available to purchase via Buysite at Staples.



IronKey

IronKey USB - Uses strong hardware-based encryption. Waterproof and tamperproof.

Deletes data after 10 failed access attempts. Compatible with any operating system, www.ironkey.com.

Available to purchase via Buysite at Staples.

Encryption Poster Posting Contest

Help the University of Chicago's Biological Sciences Division employees become aware of our Encryption tools by entering the Encryption Poster Posting Contest. Print and post the following poster throughout your workspace and send us photos of the postings to security@bsd.uchicago.edu by **September 25, 2015** to be entered into a random drawing. One winner will be selected to win a \$250 Amazon Gift Card. The more you post the greater chance to win!

[BSD ISO Encryption Poster](#)

What to do if you become aware of an information security incident?

Contact the BSD ISO Team via email at security@bsd.uchicago.edu.

Information Security Office Team

Plamen Martinov, Chief Information Security Officer	O: 773-834-1714	pmartinov@bsd.uchicago.edu
Kim Cooke, IT Security and Compliance Analyst	O: 773-834-7897	kcooke3@bsd.uchicago.edu