All About Encryption

According to the Ponemon Institute, 600,000 laptops are lost or stolen at US airports every year. The consequences of unencrypted, lost data include fines, identity theft, compromised research data, endangered federal grant status, loss of commercialization properties, erosion of alumni and donor trust, and risk to the reputation and image of the organization.

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
- E-mail
- USB Flash Drives
- Mobile devices

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

Go to security.bsd.uchicago.edu/encryption for more information on How to encrypt your devices

University of Chicago | Biological Sciences Division | BSD Information Security Office | Research-Centric Information Security Enablement Program
|E-mail: security@bsd.uchicago.edu | http://security.bsd.uchicago.edu

THE UNIVERSITY OF CHICAGO MEDICINE & BIOLOGICAL SCIENCES

Enable • Protect
RISE
Research-centric Information Security Enablement Program