Creating a Research Data Security Policy at UNC

Jane Monson

Digital Initiatives Librarian

University of Northern Colorado

http://digitalbevaring.dk/

Key Participants

- Assistant Vice President for Research
- University CIO
- Director of Technology Systems and Services (IM&T)
- Security Analyst (IM&T)
- Director of Sponsored Programs
- Dean, Associate Dean of University Libraries
- Director of Education Innovation Institute
- Faculty member in Applied Statistics and Research Methods

Background

- Growing awareness of need for systematic approach to research data management on campus
- Guidelines needed to protect personally-identifiable information resulting from research involving human subjects, in keeping with funder requirements
- Used existing policy from Harvard as model

5 Levels of Data Security

- Level 1: De-identified research information about people and other non-confidential research data
- Level 2: Benign information about individually identifiable people
- Level 3: Legally protected sensitive information about individually identifiable people
- Level 4: Very sensitive information about individually identifiable people
- Level 5: Extremely sensitive data about individually identifiable people

Overview

- Level 1 has no security requirements except that the researcher must apply for IRB approval

- Levels 3-5 are considered "sensitive research data" and require that the project investigator prepare a data security plan; researchers must undergo training in information security

- Level 2 has 16 security requirements, Level 3 has 27, Level 4 has 38, Level 5 has 47

Types of Requirements

- Physical security
  - Controlling access to physical sites where data are stored, acceptable means of data storage/sharing, data collection protocols, data backup/disposal

- Network security
  - User accounts/authorization, passwords, firewalls, antivirus software, system logs/patches, security incident handling

- File security
  - Data encryption

Future Steps

- Establish a group to continue to address data management considerations

- Integrate digital repository more fully into data management program

- Consider processes to allow future researchers access to restricted data

- Consider processes for long-term data preservation

Download the Policy

http://www.unco.edu/research/conduct.html