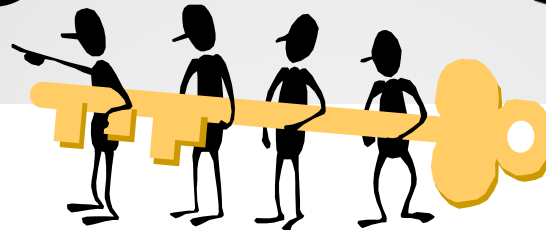# secureHeller

Addressing Information Security at Heller

October 16, 2013

Welcome to the secureHeller, the program focused on addressing Heller's information security.

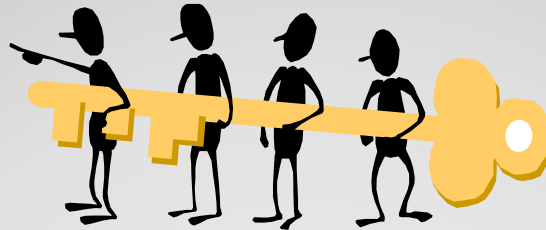**Security Awareness**

Data Protection Tools

secureHeller

Simplified Usability

Network Protection Tools

Security Awareness

secureHeller

Our key focus is to educate the Heller community, including all staff, faculty and students, on information security concepts through various channels including user training and web-based tools.

Annual User Training for Information Security
Training will be provided for every Heller user. Will include overview of Policies and Processes and will touch on all of the major areas of information security.
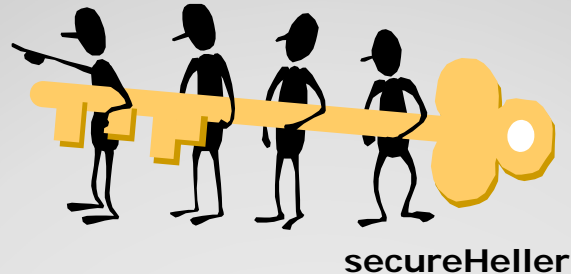
Code of Conduct
Each Heller faculty, staff and student will be responsible for reading the Security Policy and signing the Code of Conduct.

Periodic Updates
The Information Security Policy manual and other frequently used documents will be available online at myHeller to all students, faculty and staff.

Simplified Usability

secureHeller

The key focus of this Information Security initiative is to provide value to the Heller research community through improved security for research data, assurance to our funders and an enhanced Data Management Plan.

Data Management Plan
Robust data privacy protections for original physical research media and any copies, including maintaining an inventory of data files and managing physical access to them for the duration of each Data Use Agreement (DUA).

Centralized Documentation
Data Use Agreements (DUA's), Certificates of Disposition (COD's), Chain of Custody for Physical Media, et al will be maintained centrally at Heller.

Proposal Support
The Heller Information Security Policy is available on myHeller, for use in proposal writing, and will provide assurance to funders. Other frequently used documents are on myHeller, including Data Destruction Policy and Certificate of Disposition.

Data Protection Tools
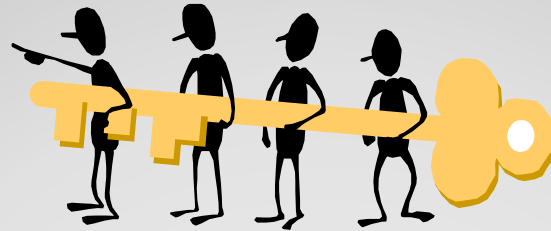
secureHeller

Our key focus is to protect both Heller's data and funders' data that is housed on individual workstations.

Secure Data Center
The on-site data center is locked at all times. Only authorized personnel can access the room using an identification card reader Our safeguards comply with the Physical Security Requirements and Best Practices for NIST/HIPAA/ISO27002.

File Backup and Storage
The Heller community has access to file storage that is backed up twice a day on the Heller file share. However, sensitive information should not be stored on the file share. For sensitive information we can back it up in the secure domain on a project by project basis.

Encryption Software
If research projects require encryption, the secureHeller group can provide full disk and removable media encryption.

Network Protection Tools
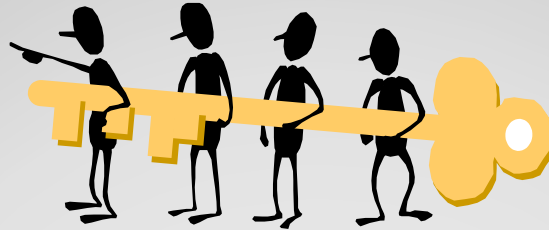
secureHeller

The goal is to protect Heller servers and clients from network intrusions and attacks.

Server and Internet Firewalls
Protect Heller's stored data from incoming threats.

Incident Management Framework
Defines what is a security incident and what steps need to be taken.

Network Administration
Recent hire of a Heller network administrator. There is an ongoing partnership with LTS to work with Heller. Support includes dedicated Heller ticket queue for issues.

VDI - Virtual desktop infrastructure
In the secure research environment, we are now using virtual desktops which allow Heller Researchers to work in an isolated secure environment for confidential data. Authorized users will be able to interact with and manipulate confidential data, while providing a high degree of assurance against data loss.

Next Steps

secureHeller
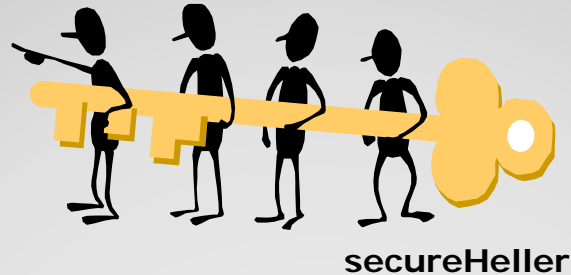
1. Read the Information Security Policy on myHeller at heller.brandeis.edu

2. Sign the Code of Conduct and give to Debbie DeWolfe – Schneider cube 222

3. Look for Information Security documents on myHeller webpage

4. Feel free to share comments and suggestions – this is a living document

5. Questions?