The INFORMATION Security Policy of The

HELLER SCHOOL FOR Social Policy and Management



**Effective Date September 20, 2012**

The INFORMATION Security Policy of The

HELLER SCHOOL FOR Social Policy and Management

Table of Contents

1. Executive Summary
   1. Compliance Statement
   2. Security Program Framework
2. Data Management Policy
   1. Possession and Storage of Data Files
   2. Data Sharing, Electronic Transmission, and Distribution
   3. Data Reporting and Publication
   4. Completion of Research Tasks and Data Destruction
3. Data Stewardship and Custodianship
4. Information Security Standards and Policy
5. Appendices
   1. Definitions
   2. Specific Laws and Regulations
   3. Policy Details
6. Forms

**1. Executive Summary**

The Heller School for Social Policy and Management (“Heller School” or “Heller”) has developed and implemented an Information Security Program that meets both the applicable requirements of Brandeis University Information Security Plan (the “Plan”) and the applicable requirements of federal and non-federal funding partners, in accordance with business requirements and relevant laws and regulations. The Brandeis plan can be found at http://lts.brandeis.edu/techhelp/content/information-security-plan.html.

The objective of this policy is to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations. Heller developed these controls based on industry best practice, Heller's existing security policies, and the internationally recognized standard, ISO 27002, as a security framework.

The controls are risk-based, and data are classified as follows: General business data for use within Heller are considered as **Level 1** data, and are protected at a baseline level of control (available to the Heller community via authenticated IT access, or authorized physical access to Heller facilities). Confidential data which can only be shared with individuals deemed to have a 'need to know' as defined by the data owner, are considered **Level 2**. This classification includes most of Heller’s current research data, and includes Limited Data Sets. Strictly Confidential are confidential data of the highest level of sensitivity, considered as **Level 3** data. FERPA, PII, PHI, PCI, and HIPAA-identified data are considered Strictly Confidential data.

Each Principle Investigator (PI) will be responsible to risk-assess their information using this rating scale, and guidelines provided by Brandeis University Information Security Plan. This Information Security Plan (the "Plan") describes Brandeis University's safeguards to protect *confidential personal information*. A copy of the Plan can be found at: http://lts.brandeis.edu/techhelp/content/information-security-plan.html

Heller researchers work with limited data sets which are considered Confidential data and are HIPAA-defined as data sets without the 16 direct identifiers but may include dates, geographic location (not as specific as street address) and any other code or characteristic not explicitly excluded. Limited data sets require a Data Use Agreement between the institution and the investigator. The Heller School does not currently work with Personal Identifiable Information (“PII”) which is considered Strictly Confidential. However, Heller researchers may work with PII in the future, so it has established security safeguards for PII. It should be noted, however, as of today, the Heller School will never be a covered entity per the Health Insurance Portability and Accountability Act (HIPAA) and therefore will not need to be compliant with those aspects of HIPAA.

All authorized users (including, but not limited to, Heller School personnel, temporary employees, interns, students, employees of independent contractors, and any applicable External Parties) of the Heller School must comply with all policies, standards, processes, and procedures created in support of this program.  Users who violate this policy will be subject to loss of access to information resources and may be subject to other disciplinary actions.

**Compliance Statement**

Heller is committed to a research compliance program, as outlined in this document. This document includes policies, procedures, and standards-of-conduct that promote adherence to applicable laws, as well as to the requirements of federal, state and private funding agencies.  The program also provides education to help faculty and research administrators stay current with the changing compliance landscape.

# 

# Security Program Framework

The security program framework includes the Security Policy, Standards, and Procedures that makeup the overall Security Program. The framework also includes a management support structure, and the specific roles and responsibilities of all resources that are required to operate, support, and maintain the security of the regulated research environment.

The Heller School will utilize the National Institute of Standards and Technology’s Risk Management Framework as their methodology. In addition, the Heller School will be responsible for:

* Ensuring compliance with laws and regulations while conducting research projects which utilize information protected by federal, state, or municipal laws or regulations, whether they are funded by government grants, private grants, or other sources;
* Making risk decisions related to actions associated with incident management activities (breaches, investigations, improper use of resources, etc);
* Monitoring compliance with legal and/or regulatory requirements (controls);
* Correcting operational activities that deviate from the security standards;
* Directing an independent assessment of the operations and technology of its secure research environment; and
* Management Direction & Support to ensure that all users involved in research projects are provided with security training and awareness, a secure physical working environment, and a secure technology resources environment.

The policy details for each of these objectives can be found in Appendix III at the end of this document.

**2. Data Management Policy**

The data management policy contains four steps. The chart below describes the four steps of the data management plan and the corresponding data privacy safeguards.

| DATA MANAGEMENT PROCESS | DATA PRIVACY AND SECURITY SAFEGUARDS | | |
| --- | --- | --- | --- |
| Organizational Safeguards | Personnel/Staffing Safeguards | Technical Safeguards |
| Possession and Storage of data files |  |  |  |
| Data Sharing/Electronic Transmission |  |  |  |
| Data Reporting/Publication |  |  |  |
| Completion of Research Tasks and Data Destruction |  |  |  |

The safeguards are designed to be reasonable and appropriate, based on the Heller organizational environment, and on NIST SP800-53 Rev 4 Draft, HIPAA Privacy, Security, Breach, and Enforcement Rules, and specific DUAs, if applicable. The safeguards describe the protections in place, and include a self-assessment document, the Heller School Self-Assessment, a copy of which is in the Forms section; see Form 4.

**POSSESSION AND STORAGE OF DATA FILES**

Heller has 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).

**Organizational safeguards policy and process**

* The DUA tracking process includes managing and maintaining an inventory of the data files and keeping it up to date.
* When original physical data arrives at Heller, it is received by the Data Custodian and logged

into the DUA log by media type.

* The physical data is then labeled with the DUA number and installed on the appropriate analytic computer.
* The physical data is then stored in a locked storage room.
* Physical data is destroyed when the project is complete by methods described in the Data Destruction Plan.

**Personnel/staffing safeguards policy and process**

* Heller requires each PI and each researcher to read and sign a Security Implementation Guidelines- Code of Personal Conduct for PI’s and Researchers document that outlines the data safeguard process. This document is in the Forms section of the Security Policy;
* Principal investigators or their designees are responsible for notifying the data manager when there is a staffing change to a project (either the addition of a new person, or someone leaving the project team;
* All project staffing changes are recorded on the DUA tracking database, and DUAs are amended to reflect these staffing changes
* Research team is trained to ensure data protection and to understand stewardship responsibilities – all Heller research personnel are required to take the Federal Information Security Awareness Training (created by the federal government to train contractors on handling and protecting the security and privacy of government data). All researchers must complete Collaborative Institutional Training Initiative (CITI) training on the projection of human subjects.
* All staff must complete and submit the certificate of completion for these trainings on an annual basis.

If there are any staffing changes from the original DUA, the Data Manager notifies a network administrator to change permissions in accordance with the written request. No one is granted permission to access a computer with Confidential data unless that person is on the DUA for that Confidential data. When someone leaves a project, that person’s permission to access the data must be revoked.

In addition, physical access to the data center is restricted. Access to data center is granted only to authorized users whose job responsibilities require access. This includes network administrators and authorized IT professionals.

In the proposed research, the data management plan will limit access to/distribution of research data files to individual (s) under a single administrative supervisor or PI.

The data management plan anticipates distributing and/or sharing research data files 1) among individuals within Heller, or 2) across one or more distinct organizations, if Partner organizations are on the DUA.

**Technical and physical safeguards policy and process**

The analytic computers with the data files are stored in a secure data center at the Heller School or at a secure data facility that is off-site. The on-site data center must remain locked at all times. In order to enter the room, there is an identification card reader that must be accessed correctly. Only authorized personnel will have the ability to access the room. In addition, there will be camera surveillance of the room. These safeguards comply with the Physical Security Requirements and Best Practices for NIST/HIPAA/ISO27002.

Within the room, the analytic computers are in an environment with a separate cooling system, an uninterrupted power supply, and redundant network access. These environmental elements are monitored.

Physical security systems comply with applicable regulations such as building codes and fire regulations.

The network, including the software, firewall, and user domain, complies with industry standards and Brandeis University standards.

* Safeguards are in place to limit access to Personal Identifiable Information (PII) among the research team, such as analytical data extracts.
* Written policies and procedures ensure that data are protected when contained on both servers and local workstations, as well as hard media devices (CDs, DVDs, hard drives, etc.), and standards for the physical removal, transfer, and destruction of data (see Form 5 DUA - Certificate of Disposition for Data).

**DATA SHARING, ELECTRONIC TRANSMISSION, AND DISTRIBUTION POLICY AND PROCESS**

Heller has the following policies to ensure privacy and security safeguards for data sharing,

electronic transmission, and distribution of data among members of the Heller community and research partners, including individuals and companies who have contractual relationships with Heller.

Protecting electronic transfers of Confidential and Strictly Confidential PII and PHI data are important aspects of the Heller Information Security program. Electronic transfers can be internal (LAN based) within the Heller School or involve external entities (WAN or internet based). Electronic transfers can be executed within batch programs, interfaces, file transfers, e-mail attachment or using physical media such as tapes or CDs. The security policies of Heller apply to all platforms, mainframe and non-mainframe environments. Standards and procedures from platform to platform complement each other, and ensure that traceability is maintained throughout the infrastructure.

Encryption is the most efficient and effective means of protecting Confidential and Strictly Confidential, PII or PHI data. Federal regulations require Heller School to protect the transmission and transport of all Confidential and Strictly Confidential PII or PHI data across external (WAN or internet based) communication paths. The transmission or transport of Confidential and Strictly Confidential PII or PHI data across internal (LAN based) communication paths are always encrypted. Any data transferred to an external storage devise must also be encrypted. This way, all Confidential and Strictly Confidential data at rest will be encrypted also (files, databases, backups, storage, etc.)

**Organizational safeguards policy and process**

Policy and procedural safeguards are in place to protect research data. These include:

* Only analysts with DUA permission to specific research data are allowed to have a single copy of the data on a secure workstation housed in the secure domain in the data center at Heller
* Within the secure domain files can be exchanged between machines. However, identified data can never be exported outside of the secure domain
* The project team also maintains one secure back-up of the original files (if this is an external hard drive and the data are encrypted).
* Analysts back up their programs used to create analytic files, but do not propagate multiple copies of their analytic files.

In addition, to track the access and use of research data, Heller maintains a DUA database which contains a list of covered data sets and authorized users. This database also tracks which machines hold which Confidential and Strictly Confidential data sets, and when data are destroyed at the conclusion of a research project.

For Individual Accountability, access to these data sets will be recorded electronically through the technology audit systems. The Heller School will use Windows access logs to ensure proper authority and access of the data. For more detailed information, please see the Appendix III.

Collaborators from an outside institution or graduate students are able to access Level 2 data if they have signed the DUA. In this case, all Heller policies in this document apply to the outside or student analyst. If individuals from a collaborator or funder organization have not signed the DUA, they may only see

de-identified data.

**Personnel/staffing safeguards policy and process**

Access to research data is governed by the Heller Principal Investigator who either distributes data or delegates this task to a lead analyst. The Principal Investigator requests that a network administrator create the necessary accounts to access the data. Should an analyst no long be involved in the project, the Principal investigator asks the administrator to remove the account. All these individuals are on the DUA. Any staffing change is tracked closely and should be reported to the DUA database administrator.

In addition to a single analyst or individual accessing particular data, the Heller School may utilize multiple simultaneous users, who may work in one or more physical locations. This situation is relatively common and needs to be accommodated.

**Technical and physical safeguards policy and process**

Access to research workstations and servers is limited, as all equipment is stored in a secure data center at the Heller School or in locked offices. (Please see above for detailed description of physical safeguards).

In addition, in order to ensure data security, there is a separation of duties and the Heller Data Security Administrator follows a password management system that includes staff authentication protocols, as well as log-on/log-off protocols. Analysts generally access workstations through the Brandeis secure VPN, which require a valid Brandeis User ID and password. These remote users utilize dual factor authentication. Once inside the Brandeis network, each user must log on to the specific data analysis workstation using a different account and unique, complex password. This password is randomly generated for dual-authentication purposes. Analysts are required to lock their machines and office door when they leave their office, so that machines are not left unattended at any time. As a secondary protection, machines time out after 15 minutes of inactivity.

The Heller data management plan proposes to store and maintain all original and backup research data files (and any derivatives made thereof for analytical use) on standalone, non-networked computer(s) in the secure data center.

All shared data and electronic transmissions will be encrypted using a secure File Transfer Protocol. In addition, Heller uses TrueCrypt, a free, open-source disk encryption software for Windows 7/Vista/XP, Mac OS X, and Linux, for whole disk encryption. The software provides many security features, including a pre-boot authentication feature.

To better safeguard the Heller IT and data resources, we have implemented the following practices. The most important practices are highlighted here. Please see Appendix III beginning on page 21 for more details.

**Desktops/laptops/end-users**

* Restrict user privileges to the filesystem and system processes. Evaluate each user’s administrator access.
* Develop and utilize an operating system update (patch) management solution. At very least, daily auto-update should be active for operating systems.
* All systems should have antivirus software installed, running, and set for daily automatic updating.
* All systems should have personal firewalls (Symantec, Windows XP firewall, MacOS X firewall, etc.) installed and running.
* All systems should have anti-spyware tools installed, running, and set for daily automatic updating.
* Users should not be allowed to create local shares on their desktops. They should only use fileserver shares.
* Confidential and Strictly Confidential Word and Excel docs should be password protected.
* Accounts with administrative privileges that are common among a group of systems should not have the same password on all the systems. Every system should have a unique password for its administrator accounts.
* Implement password-protected screen savers that activate after no more than fifteen minutes of inactivity.

**Data Sharing outside Heller**

* Review security of the external agency by the Heller Research Committee
* Consider the security of the transport and storage of data when it is shared.
* All shared media will be encrypted as described above.
* Have documentation from any external agencies that shows commitment to the security of the data being shared. Each partner organization must sign DUA and Data Destruction Policy documents.

**User Training**

The Heller School will train all new users within 60 days of employment at Heller, and will refresh the training of all existing users on an annual basis. Yearly security awareness training to include (but is not limited to):

* attachment awareness
* phishing awareness
* do not send Confidential and Strictly Confidential data via email without encryption
* password-protect Word and Excel docs.
* store Confidential data at appropriate locations (i.e., servers instead of individual desktops)
* NEVER store Confidential data on a Heller shared drive on the network
* never, under any circumstances, share a password with anyone for any reason

In addition, all new University employees are required to attend New Employee Orientation conducted by the Human Resources department. This training includes elements of safe and appropriate Information Security policies.

**Reviews and assessments policy**

Heller will develop a self-assessment methodology to make sure the security procedures are being followed. The assessment will include checks on the process, documentation, network, equipment, et. al., as per NIST Special Publication (SP) 800-53 Rev 4 Draft. Self-assessment is a very important part of this security policy, and the procedures that are put in place must be tested regularly to ensure that they are being followed and are effective.

NIST Special Publication (SP) 800-53 Rev 4 Draft, Security Self-Assessment Guide for Information Technology Systems, utilizes an extensive questionnaire containing specific control objectives and techniques against which an unclassified system or group of interconnected systems can be tested and measured. Some of the steps include: preparation for security control assessments by assuring the cooperation and collaboration of all parties having a vested interest in the security status of the organization’s information systems. Issues to be addressed include costs, schedules, and the time frame for the performance of the assessments; developing security assessment plans that will provide the objectives for the security control assessment and produce a detailed roadmap of how to conduct such an assessment; carrying out the assessment plans in accordance with the agreed-upon milestones and schedule. The assessor’s findings should be unbiased and factual in reporting what was found concerning each security control assessed; and finally, analyzing assessment reports and conduct follow-on activities. The results of the security control assessment influence the organization’s security plan and its plan of action and milestones.

Periodically, in order to evaluate the secure environment, Heller will utilize/employ an impartial third party to make sure there is a separation of duties and responsibilities. This review will occur a minimum of every two years.

**DATA REPORTING AND PUBLICATION POLICY**

Heller takes the utmost care to ensure that all analysis, findings, presentations, reports, and publications adhere to specific requirements of the DUA. The principal investigator is responsible for

requesting approval from sponsors, in writing, prior to publishing study findings that include statistics, or detail-level data to the public when this is required in the DUA.

**COMPLETION OF RESEARCH TASKS AND DATA DESTRUCTION**

The Heller School’s policy is to manage research team changes, access changes, data retention, and data destruction.

**Permissions – Giving and Removing policy and process**

The Heller School establishes rules necessary to give permission to users, and to remove permission when the users leave the school, or leave a research project. The PI is responsible for notifying the University network Administrator and the Administrative Point of Contact of any changes to the DUA.

In order to have checks and balances, these permissions are given and removed by a University network administrator, so there is a distinct separation of duties. In addition, the Administrative Point of Contact will monitor and manage the database of DUA and researchers to ensure that all researchers with permission have signed the DUA Addendum, and that only researchers with permission will be allowed access to research data files.

**Data Location, Tracking, and Destruction policy and process**

Each Principle Investigator (PI) is responsible for notifying the Administrative Point of Contact (“Admin POC”) of any changes to the DUA, so that he/she can manage and update the DUA database. Included in the DUA database are the title of the research, the DUA number, the date the research was authorized, the date the research expires, the status of the data – whether open (in use), renewed, or destroyed – and the location of the data. In addition, the DUA database contains the names of the authorized users of each research project and the DUA Addendums signed by each researcher.

All data that is used for Heller sponsored research is tracked in the DUA database, which is maintained by the Administrative Point of Contact. The location of the data, the number of copies (if applicable), the status of the DUA, and the authorized users are all tracked in this same DUA database.

Heller has policies and procedures in place to destroy the data files upon completion of the research, and has safeguards to ensure the data are protected when researchers terminate their participation in research projects. The PI is responsible for notifying the Admin POC of the disposition (including destruction) of the data. The Admin POC keeps a database of the disposition of all data. PI is also responsible for notifying the funder of the disposition of the data.

Please see Appendix IV for a copy of the Certificate of Disposition.

**At completion of a project, Heller organizational safeguards include:**

* Changes to the research team are managed with a DUA log system, and all project staffing changes are communicated to funders.
* Termination of, or removal of staff include conducting staff exit meetings. The same process applies to partner organizations that we collaborate with for a particular project
* The research security administrator is notified, and will block access to research staff or partner organization to all permitted data resources used for a completed project study and expired DUA

**Personnel/staffing safeguards include staff exit/termination policies, processes, and other external organizations, such as:**

* Meetings conducted with exiting staff to debrief, and ensure that they understand current privacy and security protection protocols
* All access to data storage and research facilities are terminated at that time
* Departing Investigators **-** When an investigator leaves Heller, (s)he recognizes that the institution must have access to the data. It is neither feasible nor desirable for the original research records to remain at the originating institution, but departing investigators must understand that they have an obligation to hold these data in trust for the institution and that such data must be returned to the institution if requested for a period of three (3) years after submission of the final report on the research project for which the data were collected, unless a longer retention period is specified by the sponsor.
* Investigators should be cognizant of the requirement to retain research data, but should recognize that certain information may be generated (for example, set-up runs, etc.) which is not research data and therefore need not be retained. Reliance should be placed on discipline-specific standards and expectations and the judgment of the senior members of the research team.

**Technical and physical safeguards include:**

* Upon completion of the sponsored research, staff no longer have access to the data files
* A Data Destruction Policy for Secure Data (see below) describes the process to ensure original data files or derivatives thereof will not be used following completion of the research project

**Data Retention Policy**

Research data generated while individuals are pursuing research studies as faculty, staff, or students of Heller, and data generated by visiting scholars utilizing the facilities of Heller, are to be retained by Heller for a period of three (3) years after submission of the final report on the research project for which the data were collected, unless a longer period is specified by the sponsor.

The original research data may be retained by the Principal Investigator on behalf of Heller but must be returned to Heller upon request of an appropriate school official. Additionally, such data must be available to representatives of external sponsors of the research or designated governmental officials, when such access is appropriate. Such data must not be disposed of during the time period referenced above unless explicit written approval for such disposition is received.

**Data Destruction Policy for Strictly Confidential Data**

1. Definitions - For the purposes of this policy, ‘Strictly Confidential data’ means any data set that contains one or more HIPAA defined identifier. These include:

* Names
* All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code, if according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000
* All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90
* Phone numbers
* Fax numbers
* E-mail addresses
* Social Security numbers
* Medical record number
* Health plan beneficiary number
* Any other account numbers
* Certificate/license numbers
* Vehicle identifiers
* Device identification numbers
* WEB URL's
* Internet IP address numbers
* Biometric identifiers (fingerprint, voice prints, retina scan, etc)
* Full face photographs or comparable images
* Any other unique number, characteristic or code.
  1. For the purposes of the policy, ‘electronic and other media’ shall include any non-paper material or media on which information can be stored or preserved, including, but not limited to, computer hard drives, zip drives, ‘thumb’ drives, floppy disks, UBS flash drives, memory sticks, magnetic tape, or other electromagnetic or electromechanical means of storing date, and includes optical storage media such as CDs or DVDs.

1. Oversight

The DUA Database Administrator has been designated as the entity responsible for oversight of destruction of secure data. The Administrator is responsible for questions regarding this policy, and should be contacted by any employee with questions regarding this policy. In addition, the Administrator shall be responsible for:

* Identifying employees who handle and dispose of secure data
* Providing training for employees regarding the requirements of this policy and the procedures for the secure destruction of secure data
* Monitoring the purchase and proper maintenance of any equipment used for secure destruction (e.g., software).
* Monitoring Heller’s compliance with this policy and applicable state and federal law regarding disposal of secure data

1. Destruction procedures for paper documents include shredding the documents using an industry-acceptable shredder, and disposing of the waste in a secure manner.
2. Destruction procedures for electronic media and other media: An employee disposing of electronic media, or non-paper and non-electronic media containing personal information shall do so by one of the following methods:
   1. Computers, servers, and portable digital assistant (‘PDA’) devices:
      1. When secure data is no longer covered by a data use agreement, all copies of those data shall be destroyed using software programs designated by the Data Security Committee or specified by the Funder. For example, CMS requires a triple swipe method for safe deletion of sensitive material. Heller operationalizes this using a program called File Shredder that can be downloaded at the following address: http://www.fileshredder.org/.
      2. The Heller standard is a data destruction method that uses a minimum of a triple swipe technique, such as File Shredder that can be downloaded at the following address: http://www.fileshredder.org/.
      3. If personal information cannot be securely erased from the device, the hard drives or other components containing the personal information shall be securely destroyed. In this situation, personal information shall be physically removed and destroyed by breaking the drive, or the drive or unit must be wiped by a suitable degaussing magnet.
   2. Zip drives, floppy disks, etc. and optical storage media:
      1. Prior to disposal, all electronic data storage media such as external hard drives, zip drives, tape drives, floppy disks, memory cards, memory sticks, USB flash drives, or other electronic storage media containing personal information shall have the data contained in the item destroyed by either wiping the media with a degaussing magnet, by using File Shredder, or by physically destroying the media through shredding or similar physical destruction.
      2. CDs, DVDs and other optical storage media must be disposed of by physical destruction of the media, such as by shredding.
3. Reporting data destruction: In order to monitor the status of secure data, Principal investigators or others responsible for the propagation of secure data must notify the DUA Database Administrator, in writing, when data destruction is complete, using the Heller Certificate of Disposition (COD) or the funders’ own COD. Principal investigators must also notify the originator of the data (e.g., CMS) when required to do so by the data use agreement. Please find a Heller Certificate of Disposition for Data (Form 5) in Section 6 Forms of this document.
4. Reports of violations: Employees should immediately notify the Heller Information Security Committee, the PI, the Brandeis IRB, and the Heller Dean of any violation of this policy, or of any concerns they may have regarding the secure disposal or destruction of secure data.

**3. Data Stewardship and Custodianship Policy**

Anyone who possesses or has access to secure research data, either electronic or otherwise, is a custodian of this data. Custodianship and its associated responsibilities apply to individuals who dispense or receive data.

Improper maintenance, disposal, or release of secure research data exposes the university to significant risk (see the "Improper Custodianship" segment of this document).

Therefore, those who request, use, possess, or have access to university administrative data must agree to certain guidelines. Below are examples of some of these guidelines in the form of general prohibitions that apply to all areas.

**General Prohibitions**

Heller staff must not access, manipulate, or change data in the following ways without prior authorization from the sponsor.

* **Note:** These examples are illustrative, not exhaustive.

- Do not circumvent the nature or level of data access given to others by providing access or data sets that are broader than those available to them via their own approved levels of access unless authorized.

- Do not facilitate another's illegal access to Heller’s administrative systems or compromise the integrity of the systems data by sharing passwords or other information.

- Do not violate university policies or federal, state, or local laws in accessing, manipulating, or disclosing secure research data.

**Note:** A data custodian must sign a Data Use Agreement

**Granting Access to Others policy and process**

Custodians of secure research data may release this data only to individuals with a legitimate interest in the data (see *"Definitions"*), and only to individuals who are either (a) employees or volunteers of the university accessing data to perform assigned duties, or (b) employees of or under contract to the university accessing data to perform special tasks, such as outside attorneys, external auditors, or other consultants.

* **Note:** Access to secure research data should be, whenever possible, to the data necessary to perform the task. In addition, the individual with the legitimate interest must remain mindful of any applicable law or policy specifically related to the handling and/or disclosure of that data

**Improper Custodianship policy**

In assuming responsibility for the interpretation and use of secure research data, custodians are expected to recognize the following potential consequences of their improper custodianship.

Suspected violations will be investigated by the appropriate office, and disciplinary measures may be taken in accordance with applicable regulations or university policy, up to and including termination. Other disciplinary action may include suspension, loss of opportunity, or loss of funding.

**4. Information Security Standards and Policy**

The following Security Standards are a sample of the control standards in ISO 27002 and NIST SP800-53 Rev 4 Draft. Since these Standards are most visible to the Heller community they are highlighted here. The full complement of Security Standards will soon be published as the Heller Security Standards Document and will include compliance with: ISO27002, NIST SP800-53 Rev 4 Draft, and the four HIPAA Security Rules.

Acceptable Use Policy

All electronic data, hardware, and software residing on the Heller School networks are considered University property (assets). All information passing through the Heller School networks, which has not been specifically identified as the property of other parties, will be treated as a Heller School asset. Unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of these resources is prohibited. For purposes of this document, the term “User” refers specifically to a Heller School Information Resources (IR) User.

Information entrusted to the Heller School will be protected in a manner consistent with its confidentiality and in accordance with all applicable standards, agreements, and laws.

Any person or entity granted access to the Heller School IR, including Heller School employees, volunteers, interns, private providers of services, contractors, and vendors must comply with the standards set forth in this document.

* Users may not attempt to access any data, program, or system for which they do not have authorization or explicit consent.
* Users must not disclose Confidential and Strictly Confidential data, or network information.
* Care must be taken to safeguard information, which is considered Confidential and Strictly Confidential, including Personally Identifiable Information (PII) and Protected Health Information (PHI). Users must ensure that Confidential Heller School materials are appropriately protected at all times.
* Any User who becomes aware of an incident of unauthorized access of confidential information must report such to the Network Administrator or Data Custodian upon discovery, generally not to exceed 24 hours.
* Users must not share their account identifiers, passwords, Personal Identification Numbers (PINS), Security/Access Tokens (e.g., Smartcards), or any other information or device used for identification, authentication, authorization, or access purposes.
* Software installed or run within the Heller School systems and/or networks must be approved by the Custodian responsible for that area.
* Before leaving their computers unattended, Users must either lock access to their workstations or logoff.
* Users of the Heller School information resources must not engage in any act that would violate the purposes and goals of Heller School as specified in its governing documents, rules, regulations, and procedures.
* Users must use appropriate safeguards to protect IR from damage, loss, or theft.
* Any User of Heller School owned or leased equipment who takes the resource off-site to an environment out of the authority of the Heller School must follow the same security policies, standards, and guidelines to protect the resource as required when in use at a Heller School location.
* All users must sign the Security Implementation Guidelines- Code of Personal Conduct for PI’s and Researchers indicating they have read, understand and agree to comply with the rules of behavior and this must be on file before any access is granted.

Account Management Policy

Account Management establishes the standards for the creation, monitoring, control, and removal of accounts. User accounts are granted to employees, partner organizations, volunteers, vendors, contractors, students and others determined who have need. These accounts assist in establishing accountability for systems use and are a key component in the protection of data confidentiality and integrity.

All partner organizations, contractors, consultants, interns or vendors, must have certain process(es) and comply with Heller Account Management standards. These organizations:

* Must have a documented process(es) to manage and modify accounts in the event of User’s termination of employment or change in job status necessitating the termination or modification of a User’s access.
* Must maintain a current list of accounts for the systems they administer.
* Must cooperate with authorized Heller School management investigating computer security incidents.
* Must restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel. Explicitly authorized personnel includes; system and security administrators, network administrators and systems programmers, database administrators or other personnel performing maintenance or system control and monitoring.

Change Management Policy

The Change Management Standard establishes a set of rules and administrative guidelines to manage changes in a rational and predictable manner, and document any changes. Changes include, but are not limited to implementation of new functionality, interruption of service, repair of existing functionality, and the removal of existing functionality. For example, any change affecting the IR computing environment (HVAC, water, plumbing, alarms, etc.) must be coordinated with the appropriate IT staff to ensure compliance with the change management process. The data custodian must review scheduled changes prior to the change. A change management log must be maintained for all changes.

Back-up and Disaster Recovery Policy

Backing up data and applications is a Heller School business requirement. It enables the recovery of data and applications in the event of loss or damage (natural disasters, system disk and other systems failures, intentional or unintentional human acts, data entry errors, or systems operator errors).

**Incident Management Policy**

The Heller Information Security Incident Management process will be invoked in the case of any potential data, system, and/or network compromises. This process will include a formal Incident Management Process such as ISO 27035 Information Security Incident Management (Industry Best Practices Framework and Standard), and will provide appropriate awareness training to users.

In the case of a security incident, the Heller Information Security Committee will be notified, along with the Data Custodian, the Heller Dean, and the University IRB.

**5. Appendices**

Appendix I - Definitions

The following are terms and definitions necessary for understanding these standards.

* + **Access** – To approach, view, instruct, communicate with, store data in, retrieve data from, or otherwise make use of information resources.
  + **Abuse of Privilege** – When a User willfully performs an action prohibited by organizational policy or law, even if technical controls are insufficient to prevent the User from performing the action.
  + **Backup** – Copy of files and applications made to avoid loss of data and to facilitate their recovery in the event of such loss.
  + **Boundary Protection** – Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection mechanisms. Protection mechanisms are devices implemented at the information system boundary and at layered or internal system boundaries, including, as appropriate, firewalls, gateways, proxies, routers and network intrusion detection systems.
  + **Change Management** – The process of controlling modification to hardware, software, firmware and documentation to ensure that information resources are protected against improper modification before, during and after implementation.
  + **Computer Incident Response Team (CIRT)** – Personnel responsible for coordinating the response to any computer security incident.
  + **Computer Security Incident** – A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. An “imminent threat of violation” refers to a situation in which the organization has a factual basis for believing that a specific incident is about to occur. For example, the antivirus software maintainers may receive a bulletin from the software vendor, warning them of a new worm that is rapidly spreading across the Internet. The terms “incident” and “computer security incident” are used interchangeably. An “event” is a negative occurrence that can be observed, verified, and documented, while an “incident” is a series of events that negatively affects the organization and/or impacts its security posture.
  + **Confidential Information** – Any information by which the identity of a client or employee can be determined either directly or by reference to other available information if the identity cannot be disclosed under federal or state law. For the purposes of this Security Policy, Confidential information is considered security **Level 2.** This classification includes most of Heller’s current research data, and includes Limited Data Sets.
  + **Consent** – Authorization to disclose identifying or other confidential information given by an individual person or entity with authority as described by law.
  + **Countermeasures** – A countermeasure or safeguard is put into place to mitigate a potential security risk exposure. A countermeasure may be a software configuration, a hardware device, or a procedure that eliminates vulnerability or reduces the likelihood of a threat agent. Examples of countermeasures include: Network Address Translation (NAT) segmentation, shielded twisted pair cabling, switched vLAN technology, fiber optic medium, IP Security (IPSec) configured for virtual private network (VPN) connections, Secure Sockets Layer (SSL), and digital certificates. Typically, countermeasures are implemented in combination or at various layers of the system’s infrastructure.
  + **Control** – A protective action, device, policy, procedure, technique, or other measure that reduces exposure of an information resource. Any method of restricting access to resources, allowing only privileged entities access to those resources. Controls include, but are not limited to, mandatory access controls, discretionary access controls, time-of-day and classification controls.
  + **Custodian** – The holder of data or agent charged with implementing the controls specified by the Owner. The Custodian is responsible for the processing and storage of information. An individual who possesses or has access to data, either electronic or otherwise.
  + **Data Classifications:**  Data with no classification are considered as **Level 1** data, which are general business data for use within Heller, and protected at a baseline level of control (available to the Heller community via authenticated IT access, or authorized physical access to Heller facilities). **Confidential**= data which can only be shared with individuals deemed to have a 'need to know' as defined by the data owner, considered **Level 2.** This classification includes most of Heller’s current research data, and includes Limited Data Sets. **Strictly Confidential=** confidential data of the highest level of sensitivity, considered as Level 3 data. FERPA, PII, PHI, PCI, and HIPAA-identified data are also considered Strictly Confidential data, classified as **Level 3**.
  + **DUA** (Data Use Agreement) - The Data Use Agreement establishes who is permitted to use or receive the limited data set and requires that the recipient agree to the following:
* Not to use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;
* Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;
* Report to the covered entity any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;
* Ensure that any agents, including a subcontractor, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; **and**
* Not to identify the information or contact the individuals.
  + **De-identify** – To remove identifiers of an individual from data as well as identifiers for the individual’s relatives, employers, or household members before it can be shared with the public. Examples of identifying data include: Name, address, social security number, phone or fax numbers, medical records and account numbers.
  + **E-mail** – Electronic mail. Any message, image, form, attachment, data, or other communication sent, received, or stored within an electronic mail system.
  + **Electronic Messaging** – The transmission of any message via an electronic means. This includes, but is not limited to, e-mail, instant messaging, wireless-broadband connectivity used in the transmission of data via hand-held devices, and/or cellular transmissions.
  + **Emergency Change** – Any immediate response to imminent critical system failure to prevent widespread service disruption.
  + **Encryption** – A method for rendering information unusable to anyone without a “key” with which they are able to “translate” the information into a readable format. The process involves translating readable data into hidden data through the use of scrambling algorithms and a “key” which permits authorized Users to unscramble the data into a useable format. When cryptography (encryption) is employed within the information system, the system must work to ensure these modules are compliant with NIST guidance, including performing all cryptographic operations using Federal Information Processing Standard (FIPS) 140-2 validated cryptographic modules with approved modes of operation.
  + **Extranet** – A private network for communications and sharing of information that, like the Internet, is based on TCP/IP, but is accessible only to authorized Users within an organization.
  + **Federal Tax Information (FTI)** – Tax return information protected by the confidentiality provisions of the Internal Revenue Code (IRC) section 6103. IRC sections 7213, 7213A and 7431provides for civil and criminal sanctions for unauthorized access of returns and tax return information.
  + **HIPAA** – Health Insurance Portability and Accountability Act of 1996, as amended, Title II includes requirements for both information and facility security compliance, and includes a Privacy Rule, Security Rule, Breach Rule, and Enforcement Rule.
  + **Incident** – Unintentional, willful or negligent unauthorized activity that affects the availability, confidentiality, or integrity of IR.
  + **Information Resources (IR)** – Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving e-mail, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.
  + **Information Resources Manager (IRM)** – The IRM is the individual responsible to the State of Texas for management of the department IR. The designation of a department IRM is intended to establish clear accountability for setting policy for IR management activities, provide for greater coordination of the state department's information activities, and ensure greater visibility of such activities within and between state agencies.
  + **Information Security Officer (ISO)** – The ISO is the individual responsible to the IRM for administering the information security program within the department. The ISO is the department’s internal and external point of contact for all information security matters.
  + **Information Technology (IT)** – The elements, structure, objectives, and resources that establish a department-level information resources management program.
  + **Institutional Review Board (IRB) at Brandeis University** - The Brandeis Committee for Protection of Human Subjects (BCPHS) is the Institutional Review Board (IRB) at Brandeis University. As such, it is charged with reviewing all research involving human subjects conducted at Brandeis University or by a member of the Brandeis community, regardless of the funding source, to ensure that the research meets with federal, state, local, and institutional regulations. Such research must be reviewed by the IRB prior to its beginning.
  + **Internet** – A global system interconnecting computers and computer networks. The computers and networks are owned separately by a host of organizations, government agencies, companies, and colleges.
  + **Intranet** – A private network for communications and sharing of information that, like the Internet, is based on TCP/IP, but is accessible only within an organization.
  + **Limited Data Set** – As an alternative to using fully de-identified information, HIPAA makes provisions for the creation of a **limited data set** which requires the removal of 16 direct identifiers but allows for the inclusion of dates, geographic location (not as specific as street address) and any other code or characteristic not explicitly excluded. This should be considered a “one-time use” data set. Limited data sets require a Data Use Agreement between the institution and the investigator and are most often utilized for retrospective chart reviews.
  + **Local Area Network (LAN)** – A group of computers and associated devices that share a common communications line. A LAN provides authentication, resources to its users, and an overall controlled inner environment.
  + **LAN User** – Any computer User with authorized access to the LAN, including applications and software.
  + **Malicious Code** – A destructive program (including virus, worm, Trojan and other malware) hidden in an attractive or innocent-looking program, application or enclosure such as a game, graphics program or screen saver.
  + **Offsite Storage** – An alternative location used for the temporary or permanent storage of data in the event that the data is unavailable at its normal site.
  + **Owner** – A person responsible: a) for a business function and b) for determining controls and access to information resources supporting that business function.
  + **Password** – A combination of letters, numbers and/or special characters that allow an authorized User id to access information within the controls defined by the information Owner.
  + **Peer-to-Peer** – Process whereby computers can trade information between each other without having to pass the information through a centrally controlled server.
  + **Personal Digital Assistants** – PDA’s include any portable computing device that is capable of transmitting data or connecting to an Information Resource. These include but are not limited to: Blackberries, Palm-Pilots, iPhones, Treo, or other similar devices, handheld devices or computers, digital or cellular phones, mobile phones or smart-phones, any web-enabled devices, portable media players.
  + **PHI** (Protected Health Information) - is information that is linked to, or could be linked to, a specific person by name, Social Security Number (SSN), date of birth (DOB), geographic area or other individually identifiable information, and is related to that person’s past, present, or future physical or mental care condition; the provision of health care to that person; or the payment for the provision of health care.
  + **PI** - Principal Investigator
  + **PII** (Personal Identifiable Information) - is any information that can be used alone or in conjunction with any other personal information to identify a specific individual. PII includes any information that can be used to search for or identify individuals, or can be used to access their records. Examples include name, SSN, DOB, Social Security benefit data, State or government issued driver’s license number.
  + **Portable Computing Device** – Any easily portable device that is capable of receiving and/or transmitting data to and from an Information Resource. They include, but are not limited to, laptop and notebook computers, handheld computers, Personal Digital Assistants (PDA’s), pagers and digital/cellular telephones.
  + **Privileged Users** - Privileged users are individuals who have access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, maintainers, system programmers).
  + **Provider** – Any individual or entity, excluding those who qualify under the definition of vendor, contracted to perform a service (typically client services).
  + **Remote Access –** Access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet) Examples of remote access methods include dial-up, broadband, and wireless.
  + **Removable Media –** Includes any storage device containing data and refers to storage media which can be removed from its reader device, conferring portability on the data it carries. For Heller School purposes, this includes removable disks or diskettes, tapes, DVD and/or compact disks (CD’s), Memory cards/sticks used in various portable digital devices, Firewire / USB “Flash/ Key/ Pen/ Thumb” drive memory devices, and any portable mass storage devices.
  + **Research data** - The recorded information, regardless of form or medium on which it may be recorded. The term includes computer software (computer programs, computer data bases, and documentation thereof), and data of a scientific or technical nature. The term does not include information incidental to award administration, such as financial, administrative, cost or pricing or management information. Scientific data include, but are not limited to, material contained in laboratory notebooks or other media such as computer disks and machine printouts. Data includes statistics, findings, conclusions, notebooks, printouts, etc.
  + **Restricted Personal Information** – Includes an individual’s social security number or data protected under state or federal law (e.g., financial, medical or student data).
  + **Risk Analysis** – The process of identifying and documenting vulnerabilities and applicable threats to information resources.
  + **Risk Assessment** – The process of evaluating the results of the risk analysis by projecting losses, assigning levels of risk and recommending appropriate measures to protect information resources.
  + **Sanitized** – Overwriting data using software tools and procedures to comply with the National Institute of Standards and Technology (NIST) Special Publication 800-88 Guidelines for Media Sanitization (SP800-88). For specific types of storage media see NIST SP800-88, Appendix A - Minimum Sanitization for Media Containing Data.
  + **Scheduled Change** – Formal notification received, reviewed and approved by a review process in advance of the change being made.
  + **Spam** – An electronic message is “spam” if: a) The recipient’s personal identity and context are irrelevant because the message is equally applicable to many other potential recipients; AND b) The recipient has not verifiably granted deliberate, explicit, and still-revocable permission for it to be sent; AND c) The transmission and reception of the message appears to the recipient to give a disproportionate benefit to the sender.
  + **Steward** An individual with the responsibility for coordinating the implementation of this policy through a) the establishment of definitions of the data sets available for access and b) the development of policies and/or access procedures for those data sets
  + **Storage Device** – Any fixed or removable device that contains data and maintains the date after power is removed from the device.
  + **Test** – A simulated or documented “real live” incident for which records are kept of the incident.
  + **Unscheduled Change** – Failure to present notice in compliance with an approved formal process in advance of the change being made.
  + **User** – An individual or automated application authorized to access an information resource in accordance with the Owner-defined controls and access rules.
  + **Vendor** – Any non-employee person or entity that exchanges goods or services (typically commercial goods and services) for money.
  + **Vulnerability Assessment** – A measurement of vulnerability, which includes the susceptibility of a particular system to a specific attack and the opportunities available to a threat agent to mount that attack.
  + **Vulnerability Report** – A computer related report containing information described in 2054.077(b), Government Code, as that section may be amended from time to time.
  + **VPN** – Virtual Private Network is a secure, private connection through a public network or an otherwise unsecure environment. It is a private connection because the encryption and tunneling protocols are used to ensure the confidentiality and integrity of data in transit. A VPN requires a tunnel to work and it assumes encryption. A tunnel is a virtual path across a network that delivers packets that are encapsulated and usually encrypted. Examples of protocols used for VPNs are: Point to Point Tunneling Protocol (PPTP), IPSec (IP Security), and Layer Two Tunneling Protocol (L2TP).
  + **Wide Area Network (WAN)** – A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more LANs. Computers connected to a WAN are often connected through public lines; such as a telephone system, and are usually leased lines or satellites. The largest WAN in existence is the Internet. A WAN provides connections between users at areas outside of a LAN through protocol tunneling and access control.
  + **Wireless Access** – Using one or more of the following technologies to access the information resources systems of a state agency or institution of higher education:

Wireless Local Area Networks – Based on the IEEE 802.11 family of standards.

Wireless Personal Area Networks – Based on Bluetooth, wireless USB, InfraRed or other limited range technologies.

Wireless Handheld Devices – Includes text-messaging devices, Personal Digital Assistant (PDAs) and smart phones.

* + **Wireless Security Guidelines** – The National Institute of Standards and Technology Special Publication 800-48, Wireless Network Security 802.11, Bluetooth and Handheld Devices.

Appendix II - Specific Laws and Regulations

NOTE: The Heller School is not a HIPAA covered entities and/or business associates, nor does it plan to become a covered entity and/or business associate. However, the Heller School understands that the HIPAA Breach Rule still applies and that Heller is not held “whole harmless” from a breach of PII and/or PHI.

The **Federal Information Security Management Act of 2002** ("**FISMA**", [44 U.S.C.](http://en.wikipedia.org/wiki/Title_44_of_the_United_States_Code)[§ 3541](http://www.law.cornell.edu/uscode/44/3541.html), *et seq.*) FISMA requires conformance to security and risk related Publications provided by the National Institute of Standards and Technology. These federal laws, regulations and standards include privacy and security requirements and supersede HIPAA privacy and security rules.

# 

# Other Applicable Federal Laws, Regulations & Standards

* FIPS 140-2 Security Requirements for Cryptographic Modules;
* FIPS 186-2, Digital Signature Standard (DSS);
* FIPS 197 AES;
* FIPS 199 Standards for Security Categorization of Federal Information and Information Systems;
* Electronic Communications Privacy Act of 1986, Public Law 99-08, 100 Stat. 1848;
* E-Government Act of 2002;
* Freedom of Information Act, 5 United States Code 552, Public Law 93-502;
* Privacy Act of 1974, 5 United States Code 552a, Public Law 99-08;
* OMB Circulars A-130 Appendix III;
* HSPD #7 Critical Infrastructure Protection;
* Medicare Modernization Act of 2003, P.L. 108-173;
* OMB Memorandum M-06-16, Protection of Sensitive Agency Information, June 23, 2006;
* NIST 800-14 (Generally Accepted Principles and Practices for Securing Information Technology Systems)
* NIST 800-16 (Information Technology Security Training Requirements: A Role and Performance-Based Model)
* NIST 800-18 (Guide for Developing Security Plans for Information Technology Systems)
* NIST SP 800-21 (Guideline for Implementing Cryptography in the Federal Government)
* NIST 800-26 (Security Self-Assessment Guide for Information Technology Systems)
* NIST 800-30 (Risk Management Guide)
* NIST 800-34 (Contingency Planning)
* NIST 800-37 (Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems)
* NIST 800-47 (Security Guide for Interconnecting Information Technology Systems)
* NIST 800-53 Rev 4 Draft (Recommended Security Controls for Federal Systems)
* NIST 800-60 (Guide for Mapping Information Systems)
* NIST 800-61 (Computer Security Incident Handling Guide)

**Appendices**

* NIST SP 800-14 *Generally Accepted Principles and Practices for Securing Information Technology* System [http//csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf](http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf)
* NIST SP 800-18 *Guide for Developing Security Plans for Information Technology Systems*[http//csrc.nist.gov/publications/nistpubs/800-18/Planguide.PDF](http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.PDF)
* NIST SP 800-26 *Security Self-Assessment Guide for Information Technology Systems*[http//csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf](http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf)
* NIST SP 800-2 *Engineering Principles for Information Technology Security (Baseline for Achieving Security)*[http//csrc.nist.gov/publications/nistpubs/800-27/sp800-27.pdf](http://csrc.nist.gov/publications/nistpubs/800-27/sp800-27.pdf)
* NIST SP 800-30 *Risk Management Guide for Information Technology Systems*[http//csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf](http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf)
* NIST SP 800-53 Rev 4 Draft *Recommended Security Controls for Federal Information Systems* http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf FIPS 199 *Standards for Security Categorization of Federal Information and Information Systems*[http//csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf](http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf)
* NIST SP 800-12 chapter 5 *An Introduction to Computer Security The NIST Handbook*[http//csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf](http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf)
* NIST SP 800-12 chapters 3, 15, 17 *An Introduction to Computer Security The NIST Handbook*[http//csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf](http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf)
* NIST SP 800-63 *Recommendation for Electronic Authentication*[http//csrc.nist.gov/publications/drafts/draft-sp800-63.pdf](http://csrc.nist.gov/publications/drafts/draft-sp800-63.pdf)
* NIST SP 800-12 *An Introduction to Computer Security The NIST Handbook*[http//csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf](http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf)
* NIST 800-88 *Guidelines for Media Sanitization*[http//csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88\_rev1.pdf](http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf)

**APPENDIX III–POLICY DETAILS**

All Heller School data in all forms (electronic, printed, or human - ie Users must not reveal protected information/data in spoken word without authenticating that the other individual(s) are authorized and have signed a DUA) must be protected. Violation of this policy may result in disciplinary action that may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of Heller School Information Resources access privileges, and to civil and criminal prosecution.

The Heller School understands that it is important to have clearly defined methods for Separation of Duties – this principle falls into a number of areas, for example: separation of access and network perspective; separation of access roles; separation of privileges; separation of requesting a user account and approving a user account, and so on.

To better safeguard the Heller IT and data resources, we have implemented the following practices:

**Departmental servers policy**

* Limit network access to servers with Edge ACLs, IPSec filtering, or some other mechanism. The rules will deny all inbound traffic except that which is explicitly permitted.
* Employ regular back-ups. Back-ups are encrypted and stored in a secure manner. Requirements for protecting backup media, and retention rules.
* Harden any services (Apache, IIS, MS-SQL, etc.) and disable any that are not necessary
* No shared usernames and passwords for any applications or servers.
* Develop and utilize an operating system update (patch) management solution. Consider whether daily auto-update should be active for operating systems.
* Perform regular reviews of file and system privileges. Develop account provisioning procedures for new hires and terminations.
* Implement password-protected screen savers that activate after no more than fifteen minutes of inactivity.
* Place servers on separate server subnets, in secure data center
* Maintain an appropriate level of logging for server OSes and applications (such as web servers). These logs should be reviewed regularly looking for indications of malicious activity.
* Implement integrity checking software, to monitor files, authentication mechanisms, and processes for unauthorized or unscheduled changes.

**Network policy**

* Implement packet filtering to protect departmental resources. This should include, at a minimum, default Edge ACLs restricting incoming connections. Firewalls can be used as well.
* For wireless networks, MAC address registration should be mandatory. No unregistered systems should be allowed on a wireless subnet.
* All systems on the network should be registered and tied to a user or network administrator.
* For wireless use, all traffic should be encrypted and have user authentication with either WPA or a VPN solution.
* Servers should be on different subnets than desktop users, and internal servers should be separated from hosts that serve data to the world.

Any connections to the Internet, or other external networks or information systems, shall occur through controlled interfaces. Protections include ensuring that only properly authorized network interconnections external to the system boundaries are established.

* + All electronic file transfers must maintain transmission integrity and confidentiality. Transmission integrity includes employing cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.
  + Encryption methods employed must meet acceptable standards. The recommended encryption method to secure data in transport is Advanced Encryption Standard 128 (AES) and Advanced Encryption Standard 256. These are encryption standards for Data Confidentiality. When cryptography (encryption) is employed within the information system, the system must work to ensure these modules are compliant with NIST guidance, including performing all cryptographic operations using Federal Information Processing Standard (FIPS) 140-2 validated cryptographic modules with approved modes of operation. SHA1 and SHA2 are the NIST Standards for Data Integrity encryption algorithms.
  + The IP address, user-id, and password used for electronic file transfers are to reside in a secure file environment. The IP address, user-id, and password must not be displayed during the execution of the job performing an electronic file transfer.

**Data Classification, Location and Tracking policy**

As mentioned in previous sections of this policy document, the research data that Heller uses in its analyses are classified as general business data or **Level 1** data, Confidential data or **Level 2** data, and Strictly Confidential data or **Level 3** data. Each Principle Investigator (PI) is responsible to risk-assess their information using this rating scale, and guidelines provided by Brandeis University Information Security Plan.

All data that is used for Heller sponsored research is tracked in the DUA database, which is maintained by the Administrative Point of Contact (“Admin POC”). The location of the data, the number of copies (if applicable), the status of the DUA, and the authorized users are all tracked in this same DUA database.

**Incident Management Standard and Framework policy**

The Incident Management Standard establishes requirements for dealing with computer security incidents. These security incidents include, but are not limited to: virus, worm and Trojan detection, unauthorized use of computer accounts and systems, and improper use of resources as outlined in these standards related to E-mail, Internet and Acceptable Use. Security incidents also include theft of hardware and/or data.

If any security incidents are detected, the individual must notify the Data Custodian, the Heller School Research Security Committee, the Dean of the Heller School, and the University IRB immediately. The University police and the Waltham police may become involved with incidents of theft.

The Heller School will audit the traffic logs on a quarterly basis to ensure appropriate use of the network, and to make sure there are no breaches or unauthorized users. In the case of a breach or unauthorized user, the auditor will notify the data custodian, Research Security Committee, the Dean of the Heller School, and the University IRB Committee.

In addition, the auditor will be a University Network Administrator, in order to have proper separation of duties and responsibilities.

**Network Access policy**

The Heller School Network Access Standard establishes security rules for the access and use of the network infrastructure.

* + - Network equipment, such as servers, firewalls, routers, switches, wireless access points, etc., shall be installed in a manner and location to prevent unauthorized access and tampering.
    - Users are permitted to use only those network addresses and access points issued to them by Heller School IT.
    - Remote Users may connect to Heller School IR using only those protocols approved by Heller School IT.

**Passwords policy**

The Heller School Password Standard establishes rules related to the User authentication process, including the creation, distribution, safeguarding, termination and reclamation of those mechanisms. Exceptions to this policy may be allowed temporarily for certain legacy systems.

All passwords must:

* + Be at least six (6) characters in length, or be eight (8) characters when technically feasible, and contain both upper and lower case characters (e.g., a-z, A-Z)
  + Have digits and special characters as well as letters,
    - Users shall commit passwords to memory and must not write down passwords and store them near their computer.
    - Users must not share their passwords.
    - If a User suspects his/her password has been compromised, he/she must change it immediately and notify his/her supervisor and the University Help Desk of the suspected compromise.

**Permissions – Giving and Removing policy**

The Heller School establishes rules necessary to give permission to users, and to remove permission when the users leave the school, or leave a research project. The PI is responsible for notifying the University network Administrator and the Administrative Point of Contact of any changes to the DUA.

In order to have checks and balances, these permissions are given and removed by a University network administrator, so there is a distinct separation of duties. In addition, the Administrative Point of Contact will monitor and manage the database of DUA and researchers to ensure that all researchers with permission have signed the DUA Addendum, and that only researchers with permission will be allowed access to research data files.

**Remote Computing policy**

The Heller School Remote Computing Security Standard establishes rules necessary to mitigate risks associated with the use of Heller School remote computing devices and their connection to the Heller School network(s).

Remote access to Level 3 or Strictly Confidential data must only be allowed when the access includes two-factor authentication. For example, this access can be accomplished via a virtual private network (VPN) connection established using Heller School issued authentication certificate(s) or hardware token.

When remote access is allowed users must also adhere to Heller School standards/policies for protecting downloaded or remote storage of confidential information. The confidential information cannot be downloaded, physically removed, or remotely stored unless authorized by the PI, or granted on a need to know basis.

When remote access to confidential information is allowed the information system must prevent further access to the system by initiating a session lock after 15 minutes of inactivity, and the session lock remains in effect until the user re-establishes access using appropriate identification and authentication procedures.

**Removable Media policy**

The Heller School Removable Media Security Standard establishes those rules necessary to protect Heller School data and networks. All Heller School portable mass storage or removable media must at a minimum be password protected or encrypted where technically feasible.

Confidential information data that is stored on removable media, and/or that is being transported to another location, must be labeled as private and confidential with a return address, be physically handed off and signed for, and tracked until it reaches its final destination.

**Security Training policy**

The purpose of the Security Training process is to ensure Users are aware of and adhere to security requirements.

* + - Users must sign the Code of Conduct Agreement stating they have read and agree to follow Heller School requirements regarding computer security policies and procedures.
    - The Heller School must provide Users with sufficient training and supporting reference materials to enable them to properly protect the Heller School IR.
    - The Heller School must develop and maintain a process enabling the communication of new computer security program information, security bulletin information and security items of interest.
    - Users must reaffirm their commitment to the protection of Heller School information resources by completing the Heller School security awareness training program on an annual basis.

The initial training will be lengthy, and will allow for a question and answer session following the training. The annual refresher training will be shorter in length. The Administrative Point of Contact will monitor and manage the database of users to ensure that all users receive proper training. All training will be conducted in the Fall, at the start of the academic year.

**Virtual Private Network (VPN) policy**

The Heller School VPN Security Policy establishes those rules necessary to mitigate risks associated with remote connections to the Heller School network(s) made by means of an approved VPN connection.

* + - All Virtual Private Networks connected to Heller School networks must be approved by the IT Security Team.
    - VPN connected equipment is subject to the same rules, policies and regulations that apply to Heller School owned equipment.
    - It is the User’s responsibility, when connected to the Heller School networks via VPN, to assure that unauthorized Users are not allowed access to the Heller School networks through the VPN connection.
    - The use of VPN access to the Heller School networks must be controlled by using password authentication, token devices or public/private key systems incorporating a strong password and/or pass-phrase.
    - VPN connections to Heller School networks must force all traffic over the VPN tunnel. All other traffic will be dropped.
    - Any computing device connected to Heller School networks or any other Heller School technology must be protected by the use of a firewall that meets the standards of Heller School.
    - Any computing device connected to Heller School networks or any other Heller School technology must use anti-virus software and configurations approved by the Heller School. Anti-virus configurations will include real time as well as passive scanning and maintain current virus definitions.
    - VPN connections will be automatically disconnected after a period of non-use or inactivity. In this event, the User must log in again. The use of any technology to maintain an inactive connection (ping, stay-connect, etc.) is prohibited and can result in termination of the VPN account.
    - The use of any VPN client other than the one provided by Heller School or its service provider is prohibited.
    - The VPN User must monitor and report intrusion or security incidents to Heller School.

**6. FORMS**

**Form 1**

University Information and Confidentiality Annual Agreement – (document pending from Brandeis)

**Form 2**

Data Use Agreement (DUA) CMS Form CMS-R-0235 (06/10) as example

**Form 3**

Security Implementation Guidelines- Code of Personal Conduct for Faculty, Staff and Students

**Form 4**

Heller School Self-Assessment - ISO 27002 Checklist

**Form 5**

DUA Certificate of Disposition for Data

**Form 6**

Annual Heller School User Training

**All the forms are posted on myHeller (login required) at:**

**http://heller.brandeis.edu/**

**Form 2**

**Data Use Agreement (CMS Form)**

**Form CMS-R-0235 (06/10) – as example only. Please see online version at: https://www.cms.gov/Medicare/CMS-Forms/CMS-Forms/downloads/cms-r-0235.pdf**

DEPARTMENT OF HEALTH AND HUMAN SERVICES CENTERS FOR MEDICARE & MEDICAID SERVICES

INSTRUCTIONS FOR COMPLETING THE DATA USE AGREEMENT (DUA) FORM CMS-R-0235

(AGREEMENT FOR USE OF CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS) DATA CONTAINING INDIVIDUAL IDENTIFIERS)

This agreement must be executed prior to the disclosure of data from CMS’ Systems of Records to ensure that the disclosure will comply with the requirements of the Privacy Act, the Privacy Rule and CMS data release policies. It must be completed prior to the release of, or access to, specified data files containing protected health information and individual identifiers.

Directions for the completion of the agreement follow:

Before completing the DUA, please note the language contained in this agreement cannot be altered in any form.

•First paragraph, enter the Requestor’s Organization Name.

•Section #1, enter the Requestor’s Organization Name.

•Section #4 enter the Study and/or Project Name and CMS contract number if applicable for which the file(s) will be used.

• Section #5 should delineate the files and years the Requestor is requesting. Specific file names should be completed. If these are unknown, you may contact a CMS representative to obtain the correct names. The System of Record (SOR) should be completed by the CMS contact or Project Officer. The SOR is the source system the data came from.

•Section #6, complete by entering the Study/Project’s anticipated date of completion.

•Section #12 will be completed by the User.

•Section #16 is to be completed by Requestor.

•Section #17, enter the Custodian Name, Company/Organization, Address, Phone Number (including area code), and E-Mail Address (if applicable). The Custodian of files is defined as that person who will have actual possession of and responsibility for the data files. This section should be completed even if the Custodian and Requestor are the same. This section will be completed by Custodian.

•Section #18 will be completed by a CMS representative.

•Section #19 should be completed if your study is funded by one or more other Federal Agencies. The Federal Agency name (other than CMS) should be entered in the blank. The Federal Project Officer should complete and sign the remaining portions of this section. If this does not apply, leave blank.

•Sections #20a AND 20b will be completed by a CMS representative.

•Addendum, CMS-R-0235A, should be completed when additional custodians outside the requesting organization will be accessing CMS identifiable data.

Once the DUA is received and reviewed for privacy and policy issues, a completed and signed copy will be sent to the Requestor and CMS Project Officer, if applicable, for their files.

2 DEPARTMENT OF HEALTH AND HUMAN SERVICES CENTERS FOR MEDICARE & MEDICAID SERVICES

Form Approved OMB No. 0938-0734 DATA USE AGREEMENT DUA #

(AGREEMENT FOR USE OF CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS) DATA CONTAINING INDIVIDUAL IDENTIFIERS)

CMS agrees to provide the User with data that reside in a CMS Privacy Act System of Records as identified in this Agreement. In exchange, the User agrees to pay any applicable fees; the User agrees to use the data only for purposes that support the User’s study, research or project referenced in this Agreement, which has been determined by CMS to provide assistance to CMS in monitoring, managing and improving the Medicare and Medicaid programs or the services provided to beneficiaries; and the User agrees to ensure the integrity, security, and confidentiality of the data by complying with the terms of this Agreement and applicable law, including the Privacy Act and the Health Insurance Portability and Accountability Act. In order to secure data that reside in a CMS Privacy Act System of Records; in order to ensure the integrity, security, and confidentiality of information maintained by the CMS; and to permit appropriate disclosure and use of such data as permitted by law, CMS and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ enter into this (Requestor) agreement to comply with the following specific paragraphs.

U.S. Department of Health and Human Services (HHS), and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

1. This Agreement is by and between the Centers for Medicare & Medicaid Services (CMS), a component of the (Requestor) hereinafter termed “User.”

2. This Agreement addresses the conditions under which CMS will disclose and the User will obtain, use, reuse and disclose the CMS data file(s) specified in section 5 and/or any derivative file(s) that contain direct individual identifiers or elements that can be used in concert with other information to identify individuals. This Agreement supersedes any and all agreements between the parties with respect to the use of data from the files specified in section 5 and preempts and overrides any instructions, directions, agreements, or other understanding in or pertaining to any grant award or other prior communication from the Department of Health and Human Services or any of its components with respect to the data specified herein. Further, the terms of this Agreement can be changed only by a written modification to this Agreement or by the parties adopting a new agreement. The parties agree further that instructions or interpretations issued to the User concerning this Agreement or the data specified herein, shall not be valid unless issued in writing by the CMS point-of-contact or the CMS signatory to this Agreement shown in section 20.

3. The parties mutually agree that CMS retains all ownership rights to the data file(s) referred to in this Agreement, and that the User does not obtain any right, title, or interest in any of the data furnished by CMS.

4. The User represents, and in furnishing the data file(s) specified in section 5 CMS relies upon such representation, that such data file(s) will be used solely for the following purpose(s).

Name of Study/Project

CMS Contract No. (If applicable)

The User represents further that the facts and statements made in any study or research protocol or project plan submitted to CMS for each purpose are complete and accurate. Further, the User represents that said study protocol(s) or project plans, that have been approved by CMS or other appropriate entity as CMS may determine, represent the total use(s) to which the data file(s) specified in section 5 will be put.

The User agrees not to disclose, use or reuse the data covered by this agreement except as specified in an Attachment to this Agreement or except as CMS shall authorize in writing or as otherwise required by law, sell, rent, lease, loan, or otherwise grant access to the data covered by this Agreement. The User affirms that the requested data is the minimum necessary to achieve the purposes stated in this section. The User agrees that, within the User organization and the organizations of its agents, access to the data covered by this Agreement shall be limited to the minimum amount of data and minimum number of individuals necessary to achieve the purpose stated in this section (i.e., individual’s access to the data will be on a need-to-know basis).

5. The following CMS data file(s) is/are covered under this Agreement.

File Years(s) System of Record

6. The parties mutually agree that the aforesaid files(s) (and/or any derivative file(s)), including those files that directly identify individuals or that directly identify bidding firms and/or such firms’ proprietary, confidential individuals, may be retained by the User until , hereinafter known as the “Retention Date.” The User agrees to notify CMS within 30 days of the completion of the purpose specified in section 4 if the purpose is completed before the aforementioned retention date. Upon such notice or retention date, whichever occurs sooner, the User agrees to destroy such data. The User agrees to destroy and send written certification of the destruction of the files to CMS within 30 days. The User agrees not to retain CMS files or any parts thereof, or specific bidding information, and those files that can be used in concert with other information to identify after the aforementioned file(s) are destroyed unless the appropriate Systems Manager or the person designated in section 20 of this Agreement grants written authorization. The User acknowledges that the date is not contingent upon action by CMS.

The Agreement may be terminated by either party at any time for any reason upon 30 days written notice. Upon notice of termination by User, CMS will cease releasing data from the file(s) to the User under this Agreement and will notify the User to destroy such data file(s). Sections 3, 4, 6, 8, 9, 10, 11, 13, 14 and 15 shall survive termination of this Agreement.

7. The User agrees to establish appropriate administrative, technical, and physical safeguards to protect the confidentiality of the data and to prevent unauthorized use or access to it.The safeguards shall provide a level and scope of security that is not less than the level and scope of security requirements established by the Office of Management and Budget (OMB) in OMB Circular No. A-130, Appendix III--Security of Federal Automated Information Systems (http://www.whitehouse.gov/omb/circulars/a130/a130.html) as well as Federal Information Processing Standard 200 entitled “Minimum Security Requirements for Federal Information and Information Systems” (http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf); and, Special Publication 800-53 “Recommended Security Controls for Federal Information Systems” (http://csrc.nist.gov/ publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf). The User acknowledges that the use of unsecured telecommunications, including the Internet, to transmit individually identifiable, bidder identifiable or deducible information derived from the file(s) specified in section 5 is prohibited. Further, the User agrees that the data must not be physically moved, transmitted or disclosed in any way from or by the site indicated in section 17 without written approval from CMS unless such movement, transmission or disclosure is required by a law.

8. The User agrees to grant access to the data to the authorized representatives of CMS or DHHS Office of the Inspector General at the site indicated in section 17 for the purpose of inspecting to confirm compliance with the terms of this agreement.

9. The User agrees not to disclose direct findings, listings, or information derived from the file(s) specified in section 5, with or without direct identifiers, if such findings, listings, or information can, by themselves or in combination with other data, be used to deduce an individual’s identity. Examples of such data elements include, but are not limited to geographic location, age if > 89, sex, diagnosis and procedure, admission/discharge date(s), or date of death.

The User agrees that any use of CMS data in the creation of any document (manuscript, table, chart, study, report, etc.) concerning the purpose specified in section 4 (regardless of whether the report or other writing expressly refers to such purpose, to CMS, or to the files specified in section 5 or any data derived from such files) must adhere to CMS’ current cell size suppression policy. This policy stipulates that no cell (e.g. admittances, discharges, patients, services) 10 or less may be displayed. Also, no use of percentages or other mathematical formulas may be used if they result in the display of a cell 10 or less. By signing this Agreement you hereby agree to abide by these rules and, therefore, will not be required to submit any written documents for CMS review. If you are unsure if you meet the above criteria, you may submit your written products for CMS review. CMS agrees to make a determination about approval and to notify the user within 4 to 6 weeks after receipt of findings. CMS may withhold approval for publication only if it determines that the format in which data are presented may result in identification of individual beneficiaries.

10. The User agrees that, absent express written authorization from the appropriate System Manager or the person designated in section 20 of this Agreement to do so, the User shall not attempt to link records included in the file(s) specified in section 5 to any other individually identifiable source of information. This includes attempts to link the data to other CMS data file(s). A protocol that includes the linkage of specific files that has been approved in accordance with section 4 constitutes express authorization from CMS to link files as described in the protocol.

11. The User understands and agrees that they may not reuse original or derivative data file(s) without prior written approval from the appropriate System Manager or the person designated in section 20 of this Agreement.

12. The parties mutually agree that the following specified Attachments are part of this Agreement:

13. The User agrees that in the event CMS determines or has a reasonable belief that the User has made or may have made a use, reuse or disclosure of the aforesaid file(s) that is not authorized by this Agreement or another written authorization from the appropriate System Manager or the person designated in section 20 of this Agreement, CMS, at its sole discretion, may require the User to: (a) promptly investigate and report to CMS the User’s determinations regarding any alleged or actual unauthorized use, reuse or disclosure, (b) promptly resolve any problems identified by the investigation; (c) if requested by CMS, submit a formal response to an allegation of unauthorized use, reuse or disclosure; (d) if requested by CMS, submit a corrective action plan with steps designed to prevent any future unauthorized uses, reuses or disclosures; and (e) if requested by CMS, return data files to CMS or destroy the data files it received from CMS under this agreement. The User understands that as a result of CMS’s determination or reasonable belief that unauthorized uses, reuses or disclosures have taken place, CMS may refuse to release further CMS data to the User for a period of time to be determined by CMS.

The User agrees to report any breach of personally identifiable information (PII) from the CMS data file(s), loss of these data or disclosure to any unauthorized persons to the CMS Action Desk by telephone at (410) 786-2580 or by e-mail notification at cms\_it\_service\_desk@cms.hhs.gov within one hour and to cooperate fully in the federal security incident process. While CMS retains all ownership rights to the data file(s), as outlined above, the User shall bear the cost and liability for any breaches of PII from the data file(s) while they are entrusted to the User. Furthermore, if CMS determines that the risk of harm requires notification of affected individual persons of the security breach and/or other remedies, the User agrees to carry out these remedies without cost to CMS.

14. The User hereby acknowledges that criminal penalties under §1106(a) of the Social Security Act (42 U.S.C. § 1306(a)), including a fine not exceeding $10,000 or imprisonment not exceeding 5 years, or both, may apply to disclosures of information that are covered by § 1106 and that are not authorized by regulation or by Federal law. The User further acknowledges that criminal penalties under the Privacy Act (5 U.S.C. § 552a(i) (3)) may apply if it is determined that the Requestor or Custodian, or any individual employed or affiliated therewith, knowingly and willfully obtained the file(s) under false pretenses. Any person found to have violated sec. (i)(3) of the Privacy Act shall be guilty of a misdemeanor and fined not more than $5,000. Finally, the User acknowledges that criminal penalties may be imposed under 18 U.S.C. § 641 if it is determined that the User, or any individual employed or affiliated therewith, has taken or converted to his own use data file(s), or received the file(s) knowing that they were stolen or converted. Under such circumstances, they shall be fined under Title 18 or imprisoned not more than 10 years, or both; but if the value of such property does not exceed the sum of $1,000, they shall be fined under Title 18 or imprisoned not more than 1 year, or both.

15. By signing this Agreement, the User agrees to abide by all provisions set out in this Agreement and acknowledges having received notice of potential criminal or administrative penalties for violation of the terms of the Agreement.

16. On behalf of the User the undersigned individual hereby attests that he or she is authorized to legally bind the User to the terms this Agreement and agrees to all the terms specified herein.

Name and Title of User (typed or printed)

Company/Organization

Street Address

City

State

ZIP Code

Office Telephone (Include Area Code)

E-Mail Address (If applicable)

Signature

Date

17. The parties mutually agree that the following named individual is designated as Custodian of the file(s) on behalf of the User and will be the person responsible for the observance of all conditions of use and for establishment and maintenance of security arrangements as specified in this Agreement to prevent unauthorized use. The User agrees to notify CMS within fifteen (15) days of any change of custodianship. The parties mutually agree that CMS may disapprove the appointment of a custodian or may require the appointment of a new custodian at any time.

The Custodian hereby acknowledges his/her appointment as Custodian of the aforesaid file(s) on behalf of the User, and agrees to comply with all of the provisions of this Agreement on behalf of the User.

Name of Custodian (typed or printed)

Company/Organization

Street Address

City

State

ZIP Code

Office Telephone (Include Area Code)

E-Mail Address (If applicable)

Signature

Date

Form CMS-R-0235 (06/10)

18. The disclosure provision(s) that allows the discretionary release of CMS data for the purpose(s) stated in section 4 follow(s). (To be completed by CMS staff.) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

19. On behalf of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ the undersigned individual hereby acknowledges that the aforesaid Federal agency sponsors or otherwise supports the User’s request for and use of CMS data, agrees to support CMS in ensuring that the User maintains and uses CMS’s data in accordance with the terms of this Agreement, and agrees further to make no statement to the User concerning the interpretation of the terms of this Agreement and to refer all questions of such interpretation or compliance with the terms of this Agreement to the

CMS official named in section 20 (or to his or her successor).

Typed or Printed Name

Title of Federal Representative

Signature

Date

Office Telephone (Include Area Code)

E-Mail Address (If applicable)

20. The parties mutually agree that the following named individual will be designated as point-of-contact for the Agreement on behalf of CMS. On behalf of CMS the undersigned individual hereby attests that he or she is authorized to enter into this Agreement and agrees to all the terms specified herein.

Name of CMS Representative (typed or printed)

Title/Component

Street Address

Mail Stop

City

State

ZIP Code

Office Telephone (Include Area Code)

E-Mail Address (If applicable)

A. Signature of CMS Representative

Date

B. Concur/Nonconcur — Signature of CMS System Manager or Business Owner

Date

Concur/Nonconcur — Signature of CMS System Manager or Business Owner

Date

Concur/Nonconcur — Signature of CMS System Manager or Business Owner

Date

According to the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number. The valid OMB control number for this information collection is 0938-0734. The time required to complete this information collection is estimated to average 30 minutes per response, including the time to review instructions, search existing data resources, gather the data needed, and complete and review the information collection. If you have any comments concerning the accuracy of the time estimate(s) or suggestions for improving this form, please write to: CMS, 7500 Security Boulevard, Attn: Reports Clearance Officer, Baltimore, Maryland 21244-1850.

**Form 3**

**Heller School for Social Policy and Management**

**Security Implementation Guidelines- Code of Personal Conduct for Faculty, Staff and Students**

For use by the Heller School faculty, staff and students to ensure that security protections are adequately implemented for information security. This document must be renewed annually.

**Please review, confirm your understanding of the following security requirements, and sign where indicated.**

1. You have read and agree to abide by the rules in the Heller Information Security Policy document, with particular attention to section 4: Information Security Standards and Policy on page 13.
2. If your research is subject to a data use agreement (DUA) you certify that the specific requirements in the DUA can be met in Heller’s secure data environment or that the research will take place in a facility which has been previously certified to meet the security requirements in the DUA.
3. You have provided a list of people (e.g. researchers, partners, etc.) with access to the research information or facility. You have provided the categories of people (e.g. IT support, facilities maintenance) that also have access to the research information or facility.
4. You agree to remove access to the research information of anyone who changes jobs or leaves the University such that they no longer require such access.
5. If remote access to the research information is required, you will ensure that the remote access is within the specifications of your DUA.
6. You agree to report a security breach, or possible breach, within 24 hours to the Heller Information Security Committee, the Brandeis Institutional Review Board (IRB), the PrincipaI Investigator (PI) on the project, and the Heller Dean. It may be necessary to involve the campus police, as well.
7. If your research protocol includes the collection of original data in the field, you must have the approval of the IRB. Prior to bringing any data into Heller, the PI agrees to comply with the Information Security Policy, including the classification of the data. The PI also agrees to the appropriate handling of Confidential and Strictly Confidential data (defined in the Heller Information Security Policy).
8. If you are the PI, you agree to destroy all original physical media at the end of the DUA per the standards in the Heller School Data Disposition Policy document.
9. If you are the researcher, you agree to destroy all derivative files containing cells of 12 or more individuals in every cell, regardless of what the rows and columns contain. For example, the derivative files must be destroyed if either the numerator or denominator is less than 12.
10. All members of the Heller community are expected to comply with the highest standards of ethical and professional conduct. You understand that willful non-compliance to the Heller Information Security Policy could result in serious Heller School consequences, and individuals may be subject to disciplinary action.

Signature of Heller faculty/staff/student\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date\_\_\_\_\_\_\_

Received by the Heller Security Research Committee Chair\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date\_\_\_\_\_\_\_

Effective date September 14, 2012

**Form 5**

**Heller School for Social Policy and Management**

**Data Use Agreement (DUA) – Certificate of Disposition (COD) for Data**

This certificate is to be completed and submitted to The Heller School to certify destruction/discontinued use of all data covered by the listed DUA at all locations and/or under the control of all individuals with access to the data. This includes any and all original files, copies made of the files, any derivatives or subsets of the files and any manipulated files. The requester may not retain any copies, derivatives or manipulated files – all files must be destroyed or properly approved in writing by Heller for continued use under an additional DUA(s). Heller will close the listed DUA upon receipt and review of this certificate and provide email confirmation to the submitter of the certificate.

**Please fill out the following:**

1. Requester Organization \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2. DUA number \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3. Please circle only one:

a. All requested files and the copies, derivatives, subsets and manipulated files have been approved by Heller for re-use. Attach a copy of the approval documentation.

b. Some requested files or copies, derivatives, subsets and/or manipulated files have been approved by Heller for re-use. Attach a copy of the approval documentation and list below the files that were destroyed.

c. No files were ever received for this DUA.

d. If All files listed below, received under the DUA listed above, have been destroyed, including copies, derivatives, subsets and manipulated files. (attach additional sheet if necessary)

FILE(S) YEAR(S)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**4. By signing this Certificate, I confirm that ALL data requested for the DUA number listed above and as applicable, copies, derivatives, subsets and manipulated files, held by all individuals who had access to, and from all the computers/storage devices where the files were processed/stored in accordance with the terms and conditions of the DUA have been properly disposed of as indicated by Section 3 above.**

5. Printed Name of Person Signing this COD \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

6. Phone # \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

7. Today’s Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

8. Email \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

9. Signature of Person Signing this COD \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Effective date September 4, 2012

Form 6

**Heller School for Social Policy and Management**

**Annual User Training for Research Security**

**User Training**

* Overview of Policies and Processes – will touch on all of the major areas, which users will read in detail and sign document that they have read and understand all of the Policies and Process in this document.
* Why we use encryption and how to use it
* Importance of unique user ids and confidentiality of authentication devices and information (2 factor authentication and password security
* Overview of Threats – social engineering, phishing, viruses and malware, down loading programs, email attachments and/or links, etc.
* Data Classifications and how to handle each classification type throughout its life cycle
* Data User Agreements – what are they and what is your responsibilities
* In process of developing using CITI training
* Q&A Session