INFORMATION SECURITY PROCEDURES FOR THE HELLER SCHOOL FOR SOCIAL POLICY AND MANAGEMENT

BRANDEIS UNIVERSITY

The Heller School FOR SOCIAL POLICY AND MANAGEMENT

Updated July 29, 2015
Version 1.1

APPROVAL:
These procedures have been approved and mandated by the following senior management:

_____

Ron Etlinger, Chief Administrative Officer, Heller School

DOCUMENT CONTROL – REVISION HISTORY

Version	Revision Date	Changes	Author
1.0	July 28, 2015	First assembled in binder	Ellen Grody
1.1	July 29, 2015	Modified language and layout	Ellen Grody
1.2	December 9, 2015	Added Chain of Custody Procedure and form	Ellen Grody
1.3	April 14, 2016	Modified Data Disposition Procedure and Certificate of Disposition	Ellen Grody

INFORMATION SECURITY PROCEDURES FOR THE HELLER SCHOOL FOR SOCIAL POLICY AND MANAGEMENT

Table of Contents

EXECUTIVE SUMMARY

METHODOLOGY AND REFERENCES

BRANDEIS UNIVERSITY

The Heller School FOR SOCIAL POLICY AND MANAGEMENT

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. These procedures are part of this Plan.

Heller senior management is committed to implementing and enforcing this Information Security Policy. This Information Security Policy is reviewed regularly, either annually, or if significant changes occur, then more often. Management approval is necessary to implement any changes to this document and to the policy.This document is owned by Ron Etlinger, Chief Administrative Officer of Heller, who has approved management responsibility for development, review and evaluation of the information security policy and procedures.

Methodology and References
The information security policy was developed by benchmarking with other universities and with the National Council of University Research Administrators.

Specifically, the following benchmarked universities and the accessed documents include (in alphabetical order):

Cornell
Cornell.edu/RAIS/ research administration information technology
Research Administration Information Services (RAIS)
RAIS Responsibility chart
Cornell Data Security Guidelines and Methodologies
Cornell Data Stewardship
Cornell Information Security
Cornell Data Stewardship and Custodianship
Cornell Recommended Security Practices for Departments and Units

Dartmouth
Dartmouth Compliance
Dartmouth PI Handbook
Dartmouth Data Management Plans – NSF
DISC (Dartmouth Information Security) Policy Control Objectives

Harvard University
Destruction of Documents
Federal and Regulatory information
HRDS (Institutional Review Board) Security Implementation Guidelines
HRDS Attestation form
HRDS Level 4 Requirements
HRDS Level 5 Requirements

Personal Medical Information

Storing High Risk Information

University of Connecticut
Code of Conduct
Incident Response
Information Security Policy Manual – Policies and Procedures
Secure File Sharing using Filelocker

DATA DISPOSITION PROCEDURE

BRANDEIS UNIVERSITY

The Heller School FOR SOCIAL POLICY AND MANAGEMENT

Data Disposition Procedure
When a project is complete and the DUA expires, the project PI must complete the Data Disposition certificate and submit it to The Heller School Information Security team (Ellen Grody egrody@brandeis.edu, Dave Reynolds reynolds@brandeis.edu and Jen Perloff perloff@brandeis.edu) 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.

The PI must testify to the disposition of 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).

The Heller DUA Administrator (Debbie DeWolfe ddewolfe@brandeis.edu) will close the listed DUA upon receipt and review of this certificate and will provide email confirmation to the submitter of the certificate.

Methods of Destruction:

Paper Documents
Destruction procedures for paper documents include shredding the documents using an industry-acceptable shredder, and disposing of the waste in a secure manner.

Electronic media and other media
Destruction procedures for electronic media and other media shall include 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/.

If secure data cannot be properly erased from the device, the hard drives or other components containing the personal information shall be securely destroyed by breaking the drive, or the drive or unit must be wiped by a suitable degaussing magnet.

Zip drives, floppy disks, etc. and optical storage media
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 secure data shall have the data contained in the item destroyed by either using File Shredder, by physically destroying the media through shredding or similar physical destruction, or by wiping the media with a degaussing magnet. CDs, DVDs and other optical storage media must be disposed of by physical destruction of the media, such as by shredding.

Audit
The Heller School Information Security team (Ellen Grody egrody@brandeis.edu, Dave Reynolds reynolds@brandeis.edu and Jen Perloff perloff@brandeis.edu) will audit the folders in the secure domain every 6 months to determine if there are project folders that have not been accessed. In those cases, the team will check with the PI to determine if the project is complete. If so, the PI will need to determine how to dispose of the data, and fill out a Certificate of Disposition.

CERTIFICATE OF DISPOSITION FORM

Heller School for Social Policy and Management

Certificate of Disposition (COD) for Data - Data Use Agreement (DUA)

This certificate is to be completed by the project PI and submitted to The Heller School Information Security team (Ellen Grody egrody@brandeis.edu, Dave Reynolds reynolds@brandeis.edu and Jen Perloff perloff@brandeis.edu) 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 the funder for continued use under an additional DUA(s). The Heller School Information Security team 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/Institute/Center _____

2. DUA number _____

3. Please circle only one:

   a. All requested files and the copies, derivatives, subsets and manipulated files have been approved by funder 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 funder 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. 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 April 14, 2016

CODE OF CONDUCT PROCEDURE

BRANDEIS UNIVERSITY

The Heller School FOR SOCIAL POLICY AND MANAGEMENT

Code of Conduct Procedure

This procedure is developed for all Faculty, Staff and Students who work at the Heller School. It outlines each person's Personal Conduct agreement for working at the Heller School. The individual must read and agree to abide by the rules in the Heller Information Security Policy.

The goal is to ensure that security protections are adequately implemented for information security. The supporting document must be renewed annually. After signing, the individual must give a copy of the document to the DUA Administrator (Debbie DeWolfe ddewolfe@brandeis.edu).

CODE OF CONDUCT FORM

BRANDEIS UNIVERSITY

The Heller School FOR SOCIAL POLICY AND MANAGEMENT

Heller School for Social Policy and Management

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.

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.

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.

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.

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.

If remote access to the research information is required, you will ensure that the remote access is within the specifications of your DUA.

You agree to report a security breach, a possible breach, or any suspected security weakness within 24 hours to the Secure network administrator and, if relevant, the Principal Investigator (PI) on the project. Depending on the nature of the event, the Heller Information Security Committee, the Brandeis Institutional Review Board, the Dean or campus police may be notified.

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).

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.

If you are the researcher, you agree to destroy all derivative files containing cells of 12 or fewer individuals or observations 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.

You agree to keep any and all data and information technology passwords confidential, and not share your passwords with other people.

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_____
Print Name_____
Received by the Heller Security Research Committee Chair_____ Date_____
Effective date May 28, 2014

PRINCIPAL INVESTIGATOR CHECKLIST

PROCEDURE

BRANDEIS UNIVERSITY

The Heller School FOR SOCIAL POLICY AND MANAGEMENT

Principal Investigator Checklist Procedure

The Heller Information Security Team has developed a checklist that a Principal Investigator (PI) of any research project can use to ensure that he/she has completed all the steps necessary to bring a new research project into Heller.

The checklist is for the benefit of the PI and does not have to be submitted to the Information Security Team. The goal is to serve as a reminder for the PI of all the steps necessary to begin a research project and store data at Heller.

PRINCIPAL INVESTIGATOR CHECKLIST FORM

BRANDEIS UNIVERSITY

The Heller School FOR SOCIAL POLICY AND MANAGEMENT

Heller School for Social Policy and Management

Principal Investigator (PI) Checklist

Following is a checklist that a Principal Investigator (PI) of any research project can use to ensure that he/she has completed all the steps necessary to bring a new research project into Heller.

Human Subjects

1. Complete IRB and submit to ORA. _____

Data Use

2. Submit copy of DUA to Debbie DeWolfe (ddewolfe@brandeis.edu). _____
3. Provide a list of people (e.g. researchers, partners, etc.) with access to the research information or facility to Debbie DeWolfe with relevant signature addendum. _____

Chartstring

4. Talk to Elaine Kennen to get the 6 digit Chartstring for your project. This will be the project identifier. _____

Remote access required?

5. If remote access to the research information is required, notify David Reynolds (heller-it@brandeis.edu) to set this up. Email should include:
    a. 6-digit chartstring (from Elaine)
    b. Authorized users with email and phone number
    c. Brief description of data and security needs _____

Data Management

6. When the data arrive:
    a. Fill out Chain of Custody form (COC) and log the data into the secure physical location. Notify Ellen Grody (egrody@brandeis.edu).
    b. If you would like to load the data yourself, use sFTP and make sure that there are no copies in an unsecure location.
    c. If your data are large or you would like help, please contact David Reynolds (heller-it@brandeis.edu) _____

Backup

7. Do you need backup for your work? If so, please contact David Reynolds (heller-it@brandeis.edu). _____

All documents referenced can be found at:

http://heller.brandeis.edu/research/secure-heller/index.html

As of May 19, 2015

INCIDENT MANAGEMENT PROCEDURE

BRANDEIS UNIVERSITY

The Heller School FOR SOCIAL POLICY AND MANAGEMENT

Incident Management Procedure

This document established the Heller School's Incident Management Procedure.

The first phase of an information security incident management process involves the detection of, collecting information associated with, and reporting on occurrences of information security events. This information must be entered into the information security incident management reporting log.

If a Heller employee detects an incident, they must fill out the Incident Management form and inform the Points of Contact (POC) Heller Network Administrator (David Reynolds reynolds@brandeis.edu) and Schneider Institutes Security Head (Jennifer Perloff perloff@brandeis.edu).

The POC will determine whether the incident should be classified as 'minor' or 'major'. In the case of a 'major' security incident, the POC will notify Ron Etlinger, Heller COO, along with the Data Custodian on the DUA (if applicable), the Heller Dean, and, if necessary, the Waltham police. (A **Major** incident is one that involves Level 3 data as defined in the Information Security Policy. Level 3 data are strictly confidential and are of the highest level of sensitivity. FERPA, PII, PHI, PCI, and HIPAA-identified data are in this category. A **Minor** incident is defined as all other incidents. These are less serious, but still reportable events. Some examples might include: Lost encrypted data, lost password.)

At this time, it will be determined if other stakeholders need to be made aware of the security incident. These could include both internal stakeholders (LTS, management staff etc.), and external stakeholders (funders, partners, etc.).

Assessing and Responding to Information Security Incidents

After an information security event is detected, reported, and the relevant information is collected, the response begins.

Assessment and decision phase

1. Determine whether the event is an actual information security incident or a false alarm. If it is not a false alarm, assess whether incident is to be classified as 'minor' or 'major'.
2. The POC also to identify the impact to individual assets, research, and applications, and the possible effects on Heller.
3. This is followed by decisions on how the confirmed information security incident must be dealt with, by whom, and in what priority.

Responding

1. Define all internal and external functions and organizations that must be involved during the management of an incident.
2. Conduct information security forensics analysis, as required.
3. Ensure that all involved activities are properly logged for later analysis, and that the information security incident management log is kept up-to-date.
4. Communicating and sharing the results of review within the Heller community to avoid similar problem in the future.

5. Communicate the information security incident and relevant details to other internal and external shareholders.
6. Identifying the lessons learned from the information security incident and vulnerabilities. This information should be used to make improvements to the organization's existing infrastructure, processes and procedures.

Once the incident has been successfully dealt with, it will be formally closed and recorded in the information security incident management log.

Resolving Incidents and Managing to a Conclusion

The POC has the responsibility for ensuring that incidents are resolved.

For the Responses phase, the POC must ensure that the key activities are followed:

- Review by the POC to determine if the information security incident is under control, and
- Investigate the required response, if it is under control. This could be an immediate response, which could include the activation of recovery procedures, and/or issuing communications to relevant involved personnel, or a later slower time response (for example, in facilitating full recovery from a disaster), While ensuring all information is ready for post-incident review activities.
- Figure out how to fix the problem. Get help from LTS or from outside consultant if necessary.
- Documentation of an information security incident, of the subsequent actions, and updating of the information security event/incident/vulnerability database.

Escalation

In extreme circumstances, matters may have to be escalated to accommodate incidents that are out of control and a potential for serious impact. In this case, the POC will confer with the Heller School COO to decide on recommended actions to deal with the information security incident.

Activity logging and change control

Activity logging is performed for all aspects of an incident, from detection to resolution, as a key for communication, accountability to ourselves and our partners, and the improvement of the system and process for everyone. The critical components of any response is in communicating the suspected or known incident as quickly as possible so decisions and responses can be made in a timely fashion.

The log contains not only the date and time of the event as well as who it was reported by, but the results of the root cause and any security forensic analysis that is pertinent.

INCIDENT MANAGEMENT FORM

BRANDEIS UNIVERSITY

The Heller School FOR SOCIAL POLICY AND MANAGEMENT

Heller School Incident Management Reporting Form

Date of Event _____ **Event Number** _____
(To be filled out by POC)

Reporting Person Information

1. Name (print) _____
2. Organization within Heller _____
3. Email and Phone number _____

Security Event Description. Please include: what occurred, how it occurred, what assets were affected.
_____

_____

_____

Was the Event **MINOR** **MAJOR**

In the case of a MINOR security incident, notify the Heller Point of Contact (POC) Heller Network Administrator (David Reynolds reynolds@brandeis.edu) and Schneider Institutes Security Head (Jennifer Perloff perloff@brandeis.edu).

In the case of a MAJOR security incident, notify the above AND the Heller COO (Ron Etlinger) along with the Data Custodian on the DUA (if applicable), the Heller Dean, and, if necessary, the Waltham police.

For Information Security Committee only:

Steps Taken to Resolve _____

Resolution of Event _____

Is response to this event closed? YES NO

If NO, when will event be closed? (Details)

Effective Date July 27, 2015

ANNUAL TRAINING PROCEDURE

BRANDEIS UNIVERSITY

The Heller School FOR SOCIAL POLICY AND MANAGEMENT

Annual Heller School Information Security Training

Training will be conducted each Fall by the Information Security Team and will include:

- 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
- Incident Management Policy
- Q&A Session

VENDOR DATA MANAGEMENT AND SECURITY

PROCEDURE

BRANDEIS UNIVERSITY

The Heller School FOR SOCIAL POLICY AND MANAGEMENT

Vendor Data Management and Security Procedure

This procedure if important when working with vendors or research partners who will be handling and accessing data where Brandeis is the Custodian. To ensure that the vendor or research partner has adequate security measures in place and appropriate data management processes, the PI or project team leader must ask the vendor or research partner to fill out the Data Management and Security Questionnaire.

Once Brandeis has received the vendor or research partner's completed Data Management and Security Questionnaire, a copy must be sent to Points of Contact (POC) Heller Security Manager (Ellen Grody egrody@brandeis.edu) and Schneider Institutes Security Head (Jennifer Perloff perloff@brandeis.edu).

DATA MANAGEMENT AND SECURITY

QUESTIONNAIRE FOR VENDORS

BRANDEIS UNIVERSITY

The Heller School FOR SOCIAL POLICY AND MANAGEMENT

BRANDEIS UNIVERSITY

The Heller School

FOR SOCIAL POLICY AND MANAGEMENT

Data Management and Security Questionnaire (DMSQ)

For xyz Company

Date

Version 1.4
May 11, 2015

1. GENERAL SYSTEM INFORMATION

a. Please identify and list all organizations, contracting companies, and government entities that are involved in providing, handling, accessing, processing, analyzing, and storing of the requested data and describe their roles.

Organization Name(s)	Role(s)

b. Please identify the physical Primary Work Location (PWL) for this project.

Primary Work Location (PWL)

2. DATA FLOW

Please complete the chart below by providing a description of how the data will be obtained and used by your organization. Of primary importance is a clear description of data flow between all parties identified above in the General System Information. Ensure data flow and associated safeguards are described. Include information about types of computer equipment used for the project (i.e., server, laptop or workstation), and information systems used to access and process data.

(In addition to this information, you may provide a data flow diagram showing the movement of data from project start to finish).

Please provide a step-by-step description of: 1. Receipt of data from _____ to your organization 2. Dissemination of data to any and all authorized users once it is received by your organization, including explanation of backup process and final reporting at the end of the project 3. Disposition of data once no longer needed for project	**Safeguards** (Please provide all technical and non-technical safeguard information for each step of the data flow).

3. DATA STORAGE at PRIMARY WORK LOCATION (PWL)

Please check all forms of data storage that will be used in this project and the physical and technical safeguards (including encryption) in place to protect them.

Type of Data Storage *(Please check all that apply)*	**Safeguards** *(Please provide information for each type of storage mechanism)*
○ Data in electronic format: o Server o Workstation o Mobile device	Do you have full disk encryption implemented on the hard drive of the devices? ○ Yes ○ No Other safeguards:
○ Data on removable media (e.g., CD/DVD, portable hard drives, USB drives, etc.)	Will you be encrypting the data stored on the removable media? ○ Yes ○ No Other safeguards:
○ Data in printed format	Will the data in printed format be protected to prevent the unauthorized access? ○ Yes ○ No Safeguards:

4. REMOTE ACCESS & ALTERNATE WORK LOCATION (AWL)

a. Will the users be allowed to work from an alternate work location (AWL) (e.g., residence, hotel, hotspot) outside of the primary work location (PWL) stated in Section 1, General System Information?

○ Yes ○ No

b. When working from the AWL, will the users have remote access to the data stored at the PWL?

○ Yes ○ No

c. Which of the following remote access methods are available to access the data from the AWL? (NOTE: Please ensure that methods for remote access are included in the data flow section).

○ Virtual Private Network (VPN)
○ Secure Socket Layer (SSL)/HTTPS
○ Secure File Transfer Protocol (sFTP)
○ Unencrypted network connection
○ Web portal access via HTTP
○ FTP

d. Please note that you are not allowed to:

○ Store data on laptops and other mobile computing devices

○ Store data on removable media (e.g., CD/DVD, portable hard drives, USB drives, etc.)

5. DATA BACKUP

a. Is the data for this project backed up?
○ Yes ○ No

b. Where/by whom is the data backed up?
○ In-House ○ Third-Party

c. Where is the backed up data stored?
○ Primary Work Location
○ Off-Site (owned by your organization)
○ Off-Site (owned by third party)

(If stored off-site, describe method of transport to off-site location).

d. What is your cycle of back-up (how often do you over-write the back-up)?

e. Please describe the safeguards in place to protect the backed up data.

f. Have you ever lost digital files? If so, explain.

g. Have you ever had version control issues? If so, please explain.

6. USER INFORMATION/DATA ACCESS

a. Please list all types of personnel who will be authorized to access data (e.g., Users, Managers, System Administrators, Developers, etc.). Please indicate the purpose in which these personnel will serve in achieving the project objective.

b. Please check **all** statements that apply to your organization:

- Authorized users with access to data have a unique user account and password.
- Level of access for each user is reviewed and granted in accordance with the required level of access needed to accomplish the project objectives.
- Our organization applies a "need-to-know" justification process in determining the level of access required for each employee and/or third party.
- Our organization has implemented policies and practices that require contractual arrangements to be made with teaming partners (organizations listed in Section 1 of this document) to ensure equal or better data protection on all shared data (inclusive of third-party vendors).

- o Our organization has implemented policies and procedures to ensure that data is not accessed by unauthorized users.

- o Our users of data for this project are on the DUA and have signed the Heller Code of Conduct.

7. COMPUTER/NETWORK TECHNICAL CONTROLS

a. The following protection devices are installed on the network (Please check all that apply):

- o Network Firewalls
- o Host based Firewalls on all workstations and servers
- o Network Intrusion Prevention/Detection System
- o System does not reside on a network

b. With regard to the system update and patching activities, please check all statements that apply to your organization:

- o Computer Operating Systems (OS) are current with the latest patches and security updates in accordance with the organization's patch management policy.

- o Anti-Virus software is deployed throughout the network on workstations and servers and is periodically updated.

- o Anti-Spyware software is deployed throughout the network on workstations and servers and is periodically updated.

c. Which of the following safeguards are implemented on workstations in the case of inactivity?

- o Automatic account log-off feature will log off the user after the predetermined time of inactivity, requiring the user to re-authenticate.

- o Automatic screen lock will be activated after the predetermined time of inactivity, requiring the user to re-authenticate.

8. PHYSICAL PROTECTION

a. With regard to physical security controls, please check the **one** statement that applies to your organization:

- o All computing resources for the project (e.g., servers, workstations, laptops) are behind locked office doors and there are other safeguards preventing unauthorized physical access to the systems.

- o Some computing resources are behind locked office doors and some workstations are not protected by locked doors (e.g. Computers placed in cubicles).

- o None of the computing resources are protected by locked office doors.

b. Please check all access controls that apply to your organization's physical protection. Please identify other access controls that apply to your organization:

- o Security guards
- o Cipher locks
- o ID Badge
- o Other:_____

9. DATA DISPOSITION (Electronic and Hard Copy)

a. Briefly describe the procedures you will use for removing data from the information system resources when no longer needed for this project. Ensure that this information is consistent with the Heller School Data Disposition policy.

b. With regard to reusable media protection, please check all policies and procedures implemented in your organization:

- o Policy/procedure on sanitizing or destroying data from disks, hard drives, and/or CDs.

- o Policy/procedure on proper disposal of printed (hard copy) data (i.e., shred or burn).

c. With regard to hardware inventory tracking, please check **all** policies and procedures that are implemented in your organization:

- o Records are created and maintained to track each instance of computer equipment issuance to individual employees and/or internal organizations.

- o Records are updated when custodianship of hardware is changed from one employee or team to another.

- o Records are updated and equipment is retrieved from each individual leaving the organization.

10. AUDIT

a. Are security audit controls implemented that record and examine user activity on the information system where the data is processed and stored?

○ Yes ○ No

b. Please specify the information system components where auditing is implemented (e.g., server, workstation, laptop)

c. For each component, please list what events and/or activities are logged and reviewed.

d. Please indicate the frequency of the review required by your policies.

11. INCIDENT RESPONSE

a. With regard to your organization's Incident Response program, please check all that apply:

- o There is a formalized organization-wide Incident Response program in place.
- o The organization's Incident Response program includes detailed response procedures for privacy breaches and security incidents involving data.
- o Employees are trained regarding their responsibilities to report incidents and have an understanding of what constitutes a privacy breach and security incident.

b. If any, please state the circumstances of network or system breaches in your organization and the courses of actions taken to restore and ensure system integrity.

12. TRAINING AND AWARENESS

With regard to employee training and awareness, please check all that apply to your organization.

- o Employees are required to receive initial and follow up refresher training periodically.
- o Training includes topics relating to privacy and security.
- o Our organization does not conduct training relating to privacy and security.

The following signatories acknowledge that the information provided in this DMSQ is truthful and accurate, and that all necessary security measures will be taken to secure all project data. By signing below, the Data Sharing Requestor understands that he/she is required to promptly notify the Heller School project PI of any change to information systems and safeguards.

Person Completing this Data Security Questionnaire:

_____

(Name and Title of Technical Representative - Typed or Printed)

_____

(Company/Organization)

_____

(Business Street Address)

_____

(City/State/ZIP Code)

_____

(Business Phone No. including Area Code/Business E-Mail Address)

_____ _____

(Signature) (Date)

Data Sharing Requestor:

_____

(Name and Title of Data Sharing Requestor - Typed or Printed)

_____

(Company/Organization)

_____

(Business Street Address)

_____

(City/State/ZIP Code)

_____

(Business Phone No. including Area Code/Business E-Mail Address)

_____ _____

(Signature) (Date)

Heller School Principal Investigator (PI):

_____

(Name and Title of Heller School PI - Typed or Printed)

_Heller School at Brandeis University_____

(Company/Organization)

_____

(Business Street Address)

_____

(City/State/ZIP Code)

_____

(Business Phone No. including Area Code/Business E-Mail Address)

_____ _____

(Signature) (Date)

Heller School Information Security Review:

_____

(Name and Title of Heller School Information Security Team Member - Typed or Printed)

_____ _____

(Signature) (Date)

CHAIN OF CUSTODY PROCEDURE

Chain of Custody Procedure

The project PI must give project data to The Heller School Information Security team (Ellen Grody egrody@brandeis.edu, Dave Reynolds reynolds@brandeis.edu and Jen Perloff perloff@brandeis.edu) to document receipt into Heller per Form 11 on following page.

Dave Reynolds loads the data into the secure data center and gives access to the data per the DUA.

Next, the data media are returned to the locked storage cabinet, and the COC form is updated.

Any time the data media are removed from the locked storage cabinet, they must be ‘signed out’.

CHAIN OF CUSTODY FORM

BRANDEIS UNIVERSITY

The Heller School FOR SOCIAL POLICY AND MANAGEMENT

Form 11

CHAIN OF CUSTODY FORM		Project ID#:	
		DUA #:	
		PI Name:	
	Data Delivery Date:		
	Data Receipt E-mailed (Y/N):		

Physical Device Description:	
Purpose of Data:	
Comments:	

From:		Date:	
Signature:		Time:	
To:		Date:	
Signature:		Time:	
Reason:			
From:		Date:	
Signature:		Time:	
To:		Date:	
Signature:		Time:	
Reason:			

BUSINESS CONTINUITY PROCEDURE

BRANDEIS UNIVERSITY

The Heller School FOR SOCIAL POLICY AND MANAGEMENT

Business Continuity Procedure

In the case of the Network Administrator being out for a period of time, the Heller School has a procedure to ensure business will continue without interruptions. The first step in implementing this procedure is to develop a plan framework and document the needs and requirements of the Heller School. Below are the critical skills and responsibilities for an outsourced Network Administrator in both the short-term and the long-term.

The next step is to find the best vendor to perform these duties, and implement a retainer contract with the vendor. **The Heller School will work on this step in the near term.**

BUSINESS CONTINUITY REQUIREMENTS

BRANDEIS UNIVERSITY

The Heller School FOR SOCIAL POLICY AND MANAGEMENT

Business Continuity Requirements

Service Level Agreement for Outsourced Network Administrator
This SLA is for a network engineer at the Heller School. The person(s) will be responsible for effective provisioning, installation, configuration, operation, and maintenance of systems hardware, software, security and related infrastructure. The person(s) will be responsible for the following:

IF NEED FOR 1-2 DAYS

1. Familiarity with Heller hardware and software, including:
    - VMware products (ESXi, vSphere, Horizon View, vCenter, Composer)
    - sFTP solution from IPSwitch
    - SecureID token installation and maintenance from RSA
    - Fortinet firewall solutions
    - HP servers, SANS, and switches

2. Perform daily system monitoring, verifying the integrity and availability of all hardware, server resources, systems and key processes, reviewing system and application logs, and verifying completion of scheduled jobs such as backups where appropriate.
    - VMware system access and performance logs
    - Review HP network appliance logs

3. Perform regular security monitoring to identify any possible intrusions.
    - sFTP access logs
    - updating black/white lists
    - Review firewall logs

IF NEED FOR MONTH OR MORE

4. Analyze, troubleshoot, and investigate security-related, information systems' anomalies based on security platform reporting, network traffic, log files, host-based and automated and manual security alerts.

5. Monitor, review and correct issues surrounding daily backup operations.

6. Account Management including:
    - Create, change, and delete user accounts per request.
    - Software used?
    - Manage user accounts as part of on/off-boarding process.

7. Apply OS patches and upgrades on a regular basis, and upgrade administrative tools and utilities. Configure / add new services as necessary.

8. Maintain data center environmental and monitoring equipment.
    - Temperature monitoring
    - Core equipment availability monitoring

Required experience and knowledge:
- Windows XP, 7, 8, 8.1, Server 2008R2, Server 2012, Mac OS X, Various Linux Distributions
- Active Directory maintenance including multiple Domains

- Mac and PC hardware, Printers, scanners, computer peripherals, Mobile devices (iOS, Android)
- Network connectivity – including Ethernet, TCP/IP, VPN, DNS, DHCP and VLAN technologies
- Network Hardware - including switches, routers and firewalls and their configurations
- HP Thin Clients, (ThinPro and WES) and HP Device Manager
- Windows file server knowledge
- Experience with Imaging tools such as Ghost
- Malware and virus detection and removal techniques
- Strong customer service and troubleshooting skills
- Ability to communicate technical information, both verbal and written, to a wide range of end-users
- Ability to work independently within a larger group of technology professionals
- Extensive VMware vSphere and Horizon View experience
- SAN configuration/maintenance
- Understanding of SQL configuration, maintenance and query language
- Network design and configuration experience
- Firewall appliance configuration and maintenance

FUTURE PROCEDURES

BRANDEIS UNIVERSITY

The Heller School FOR SOCIAL POLICY AND MANAGEMENT

Future Procedures
The Information Security Team is working on developing and documenting policies and procedures for:

Change Management
The Change Management process will be developed in the near future. This process 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 processes or forms, and so on. A change management log will be maintained for all changes.

Back-up and Disaster Recovery
Backing up data and applications will be developed in the near future. This will enable 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).