Hebrew College Written Information Security Program

Responsible office	CIT – Center for Information Technology team
Responsible party	Director of information technology
Last Save Date	2/11/21
Status	Approved
Last revision #	64th
Approved by	Data Management Team
Approval date	12/11/20
Effective date	12/11/20
Last review	2/11/21

Contents

1 Policy Statement

The Hebrew College Written Information Security Program ("WISP") is intended as a set of comprehensive guidelines and policies designed to safeguard all confidential and restricted data maintained at the College, and to comply with applicable laws and regulations on the protection of Personal Information and Nonpublic Financial Information, as those terms are defined below, found in records and in systems owned by the College.

2 Overview & Purpose

The WISP was implemented to comply with regulations issued by the Commonwealth of Massachusetts entitled "Standards For The Protection Of Personal Information Of Residents Of The Commonwealth" [201 Code Mass. Regs. 17.00], and by the Federal Trade Commission [16 CFR Part 314], and with our obligations under the financial customer information security provisions of the federal Gramm-Leach-Bliley Act ("GLB") [15 USC 6801(b) and 6805(b) (2)]. Overview of regulations are list in the Appendix at the end of this document.

In accordance with these federal and state laws and regulations, Hebrew College is required to take measures to safeguard personally identifiable information, including financial information, and to provide notice about security breaches of protected information at the college to affected individuals and appropriate state agencies.

Hebrew College is committed to protecting the confidentiality of all sensitive data that it maintains, including information about individuals who work or study at the College. Hebrew College has implemented a number of policies to protect such information, and the WISP should be read in conjunction with these policies that are cross-referenced at the end of this document.

The purposes of this document are to:

- Ensure the security and confidentiality of personal information
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information
- Protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud
- Establish a comprehensive information security program for Hebrew College with policies designed to safeguard sensitive data that is maintained by the College, in compliance with federal and state laws and regulations;
- Establish employee responsibilities in safeguarding data according to its classification level; and
- Establish administrative, technical and physical safeguards to ensure the security of sensitive data.

3 Scope

In formulating and implementing the WISP, Hebrew College has addressed and incorporated the following protocols:

- identified reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information;
- assessed the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information;
- evaluated the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks;

- designed and implemented a WISP that puts safeguards in place to minimize those risks, consistent with the requirements of 201 CMR 17.00; and
- Implemented regular monitoring of the effectiveness of those safeguards.

This Program applies to all Hebrew College employees, whether full- or part-time, including faculty, administrative staff, contract and temporary workers, hired consultants, interns, and student employees, as well as to all other members of the Hebrew College community (hereafter referred to as the "Community"). This program also applies to certain contracted third-party vendors (see section 6.7 for further information). The data covered by this Program includes any information stored, accessed or collected at the College or for College operations. The WISP is not intended to supersede any existing Hebrew College policy that contains more specific requirements for safeguarding certain types of data, except in the case of Personal Information and Nonpublic Financial Information, as defined below. If such policy exists and is in conflict with the requirements of the WISP, the other policy takes precedence.

4 Definitions

4.1 Data

For the purposes of this document, data refers to information stored, accessed or collected at the College about members of the College community.

4.2 Data Custodian

A data custodian is responsible for maintaining the technology infrastructure that supports access to the data, safe custody, transport and storage of the data and provide technical support for its use.

4.3 Data Steward

A data steward is responsible for the data content and development of associated business rules, including authorizing access to the data.

4.4 Data Security Coordinator

The Data Security Coordinator is responsible for implementing, supervising and maintaining the WISP. They are responsible for the following:

- Initial implementation of the WISP
- Regular testing of the WISP's safeguards;
- Evaluating the ability of each of our third party service providers to implement and maintain appropriate security measures for the personal information to which we have permitted them access, consistent with 201 CMR 17.00; and requiring such third party service providers by contract to implement and maintain appropriate security measures.
- Reviewing the scope of the security measures in the WISP at least annually, or whenever there is a material change in our business practices that may implicate the security or integrity of records containing personal information.
- Conducting an annual training session for all supervisors, employees and independent contractors, including temporary and contract employees who have access to personal information on the elements of the WISP. All attendees at such training sessions are required to certify their attendance at the training, and their familiarity with the school's requirements for ensuring the protection of personal information.

4.5 Personal Information

Personal Information ("PI"), as defined by Massachusetts law (201 CMR 17.00), is the first name and last name or first initial and last name of a person in combination with any one or more of the following:

- Social Security number;
- Driver's license number or state-issued identification card number; or
- Financial account number (e.g. bank account) or credit or debit card number that would permit access to a person's financial account, with or without any required security code, access code, personal identification number, or password.

For the purposes of this Program, PI also includes passport number, alien registration number or other government-issued identification number.

4.6 Nonpublic Financial Information

The GLB Act (FTC 16 CFR Part 313) requires the protection of "customer information", that applies to any record containing nonpublic financial information ("NFI") about a student or other third party who has a relationship with the College, whether in paper, electronic or other form that is handled or maintained by or on behalf of the College. For these purposes, NFI shall include any information:

- A student or other third party provides in order to obtain a financial product or service from the College;
- About a student or other third party resulting from any transaction with the College involving a financial product or service; or
- Otherwise obtained about a student or other third party in connection with providing a financial product or service to that person.

Examples of NFI include:

- Information a consumer provides to you on an application to obtain a loan, credit card, or other financial product or service;
- Account balance information, payment history, overdraft history, and credit or debit card purchase information;
- The fact that an individual is or has been one of your customers or has obtained a financial product or service from you;
- Any information about your consumer if it is disclosed in a manner that indicates that the individual is or has been your consumer;
- Any information that a consumer provides to you or that you or your agent otherwise obtain in connection with collecting on, or servicing, a credit account;
- Any information you collect through an Internet "cookie" (an information collecting device from a web server); and
- Information from a consumer report.

5 Data Classification

All data covered by this policy will be classified into one of three categories outlined below, based on the level of security required for each, starting with the highest level.

5.1 Confidential

Confidential data refers to any data where unauthorized access, use, alteration or disclosure of this data could present a significant level of risk to Hebrew College or the Community. Confidential data should be treated with the highest level of security to ensure the privacy of that data and prevent any unauthorized access, use, alteration or disclosure.

Data Classification	Risk Level	Description	Examples
Confidential	**High**	Data whose loss, corruption, or unauthorized access would pose an extreme identity or financial risk to the College, a school partner, or the public and require notification of the MA Attorney General and affected users. Confidential data includes data that is protected by the following federal or state laws or regulations: 201CMR17.00 (Mass Security Regs), 16 CFR 313 (Privacy of Consumer Financial Information), Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the FTC's Red Flag Rules. Information protected by these laws includes, but is not limited to, PI, NFI and Protected Health Information (PHI).	• Social Security Number • Credit/Debit Card Number • Bank/Financial Account Numbers • HIPAA or medical records • Passwords or Biometric data • Driver's License or State ID number

5.2 Restricted

Restricted data refers to all other personal and institutional data where the loss of such data could harm an individual's right to privacy or negatively impact the finances, operations or reputation of Hebrew College. Any non-public data that is not explicitly designated as Confidential should be treated as restricted data.

Restricted data should be limited to access by individuals who are employed by or matriculate at Hebrew College and who have legitimate reasons for accessing such data, as governed by FERPA, or other applicable law or College policy. A reasonable level of security should be applied to this classification to ensure the privacy and integrity of this data.

Data Classification	Risk Level	Description	Examples
Restricted	**High**	Restricted data includes data protected by the Family Educational Rights and Privacy Act	• Student ID

		(FERPA), referred to as student education records. This data also includes, but is not limited to, donor information, intellectual property (proprietary research, patents, etc.), College financial and investment records, employee salary information, or information related to legal or disciplinary matters.	• Employee ID • HR Documents • College Proprietary Data or Intellectual Property • Copyrighted College or Student material • Board meeting minutes • Expense reports • Litigation • Software license numbers • College infrastructure plans • System configuration/log files • Social Security Number • Credit/Debit Card Number • Bank/Financial Account Numbers • HIPAA or medical records • Passwords or Biometric data • Driver's License or State ID number • FERPA records • Training data

5.3 Public (or Unrestricted)

Public data includes any information for which there is no restriction to its distribution, and where the loss or public use of such data would not present any harm to Hebrew College or members of the Hebrew College community. Any data that is not classified as Confidential or Restricted should be considered Public data.

Data Classification	Risk Level	Description	Examples
Public (or Unrestricted)	**Low to None**	Data to which the general public has access	• Any data found on www.hebrewcollege.edu • Policies • Publications • Academic Calendar • Campus Maps

6 Policy

6.1 Responsibilities

6.1.1 Data Custodian

Director of Information Technology serves as Data Custodian

A data steward is responsible for the data content and development of associated business rules, including authorizing access to the data.

6.2 Data Security Coordinator

Director of Information Technology serves as the Data Security Coordinator.

6.3 Data Steward

All data at the College is assigned a data steward according to the constituency it represents. Data stewards are responsible for approval of all requests for access to such data. The data steward for each constituency group are designated as follows:

Type of Data Data Steward* (organized based on data that is stored in ...)

Campus Café/Jenzabar - Director, Office of Student Services

QuickBooks – Business Office Manager

Paper – VP for Finance and Administration, Director Human Resources & Departmental Managers

Website – Director of Marketing (PII should not be on website)

Electronic folders/files - Director of Information Technology

*The data steward may appoint a designee to serve in their place.

College Information Technology (CIT) staff serve as the data custodians for all data stored centrally on the College's servers and administrative systems, and are responsible for the security of such data.

Human Resources will inform CIT staff about an employee's change of status or termination as soon as is practicable but before an employee's departure date from the College. Changes in status may include terminations, leaves of absence, significant changes in position responsibilities, transfer to another department, or any other change that might affect an employee's access to College data.

Department heads will alert CIT at the conclusion of a contract for individuals that are not considered Hebrew College employees in order to terminate access to their Hebrew College accounts.

CIT is in charge of maintaining, updating, and implementing this Program. The College's Director of Information Technology has overall responsibility for this Program.

All members of the Community are responsible for maintaining the privacy and integrity of all sensitive data as defined above, and must protect the data from unauthorized use, access, disclosure or alteration. All members of the Community are required to access, store and maintain records containing sensitive data in compliance with this Program.

6.4 Identification and Assessment of Risks to College Information

Hebrew College recognizes that it has both internal and external risks to the privacy and integrity of College information. These risks include, but are not limited to:

- Unauthorized access of Confidential data by someone other than the owner of such data
- Compromised system security as a result of system access by an unauthorized person
- Interception of data during transmission
- Loss of data integrity
- Physical loss of data in a disaster
- Errors introduced into the system
- Corruption of data or systems
- Unauthorized access of Confidential data by employees
- Unauthorized requests for Confidential data
- Unauthorized access through hard copy files or reports
- Unauthorized transfer of Confidential data through third parties

Hebrew College recognizes that this may not be a complete list of the risks associated with the protection of confidential data. Since technology growth is not static, new risks are created regularly. Accordingly, CIT will actively participate and monitor advisory groups such as the Homeland Security National Cyber Awareness System, ESET Welivesecurity Newsletter and SANS Newsletters: @RISK for identification of new risks.

Hebrew College believes the College's current safeguards are reasonable and, in light of current risk assessments made by CIT, are sufficient to provide security and confidentiality to confidential data maintained by the College. Additionally, these safeguards protect against currently anticipated threats or hazards to the integrity of such information.

6.5 Policies for Safeguarding Confidential Data

To protect College data classified as Confidential, the following policies and procedures have been developed that relate to access, storage, transportation and destruction of records.

6.5.1 Access & Storage

- Only those employees or authorized third parties requiring access to confidential data in the regular course of their duties are granted access to this data, including both physical and electronic records.

- To the extent possible, all electronic records containing Confidential data should only be stored on Hebrew College's on-campus secure network storage and not on local machines, unsecured servers or cloud technology.
- Massachusetts PI and NFI must not be stored on any Google app.
- Confidential data must not be stored on cloud-based storage solutions that are unsupported by the College (including DropBox, Microsoft OneDrive, Apple iCloud, etc.).
- Members of the Community are strongly discouraged from storing confidential data on laptops or on other mobile devices (e.g., flash drives, smart phones, external hard drives). However, if it is necessary to transport confidential data electronically, the mobile device containing the data must be encrypted.
- Paper records containing confidential data must be kept in locked files or other secured areas when not in use.
- Upon termination of employment or relationship with Hebrew College, electronic and physical access to documents, systems or other network resources containing confidential data is immediately terminated. All records containing PII, in any form, must be returned at the time of termination of the relationship. If return is not feasible, destruction in accordance with industry standards, along with proof of such destruction, is acceptable.

6.5.2 Transporting Confidential Data

Members of the Community are strongly discouraged from removing records containing confidential data off campus. In rare cases where it is necessary to do so, the user must take all reasonable precautions to safeguard the data. Under no circumstances are documents, electronic devices, or digital media containing confidential data to be left unattended in any unsecure location.

When there is a legitimate need to provide records containing confidential data to a third party outside Hebrew College, electronic records shall be password-protected and/or encrypted, and paper records shall be marked confidential and securely sealed.

6.5.3 Destruction of Confidential Data

Records containing confidential data must be destroyed once they are no longer needed for business purposes, unless state or federal regulations require maintaining these records for a prescribed period of time.

Paper and electronic records containing confidential data must be destroyed in a manner that prevents recovery of the data. Massachusetts General Law 93I specifies the manner in which records containing PI must be destroyed.

6.5.4 Traveling Abroad with Students' Personal Information

In the event that transmission of student passport information is required by the hotel or program abroad in advance of the travel, only the relevant information requested (e.g., Name, Passport Number, Date of Expiry, and Date of Birth) will be provided, not complete copies of the passport images. This information should first be transmitted via fax or through eFax secure website (SSL), provided that the Hebrew College department arranging the travel confirms the accuracy of the fax number by sending an initial confirmation message before the actual data. If faxing is unavailable, the data may be sent via Hebrew College email, provided that the same confirmation of transmission takes place.

Faculty/staff who need to retain these passport numbers for arranging travel will store this data in spreadsheets that are saved on the College's server. Any spreadsheets containing student passport information should be routinely deleted by the spreadsheet owner when no longer needed.

Faculty/staff who are traveling with the students abroad that need student passport and visa information for hotel check-in will keep a paper record on their person that contains relevant information (such as the passport and visa numbers and their expiry dates) and the last names of the students only. Faculty/staff must not retain or travel with copies of student passports.

In extreme circumstances involving travel to a remote location where access to technology would be limited and would prohibit retrieval of a lost passport, a program director may request an exemption to this policy allowing for him or her to retain copies of the students passports during travel. This request will be made to the V.P. of Finance and Administration for approval. The employee and the employee's supervisor will acknowledge, in writing, their understanding of the WISP and their responsibilities in protecting the passports.

6.6 Policies for Safeguarding Restricted Data

Access to Restricted Data should be limited to members of the Community who have a legitimate business need for the data.

Restricted data may be stored on cloud-based storage solutions that are unsupported by the College as long as they are in compliance with the requirements of any laws governing the protection of such data (e.g., FERPA).

Documents containing Restricted Data should not be posted publicly.

6.6.1 Password Requirements

In order to protect College data, all members of the Community must select unique passwords following these guidelines:

- Has at least 8 characters
- Contains a combination of at least three of the four character types: uppercase and lowercase letters, numbers, and special characters (e.g. @ $ # !)
- Does not contain repeated characters or a sequence of keyboard letters (e.g., qwerty, 12345, or yyy99)
- Does not contain any part of the user's name, username, birthday, or social security or those of friends and family (e.g., Jill1030)

Members of the community must protect the privacy of their passwords. Passwords must not be shared with others. If an account or password is suspected to have been compromised, all passwords should be changed immediately and the incident reported to the Hebrew College Help Desk.

6.7 Third-Party Vendor Agreements Concerning Protection of Personal Information

Hebrew College exercises appropriate diligence in selecting service providers capable of maintaining appropriate security safeguards for PI provided by the College to them. The primary budget holder for each department is responsible for identifying those third parties providing services to the College that have access to PI. All relevant contracts with these third parties are reviewed and approved by the VP for Finance and Administration to ensure the contracts contain the necessary language regarding safeguarding PI. It is the responsibility of the primary budget holders to confirm that the third parties are required to maintain appropriate security measures to protect PI consistent with this Program and where required by Massachusetts laws and regulations 201 CMR 17.00.

6.8 Computer system safeguards

CIT staff monitor and assess safeguards on an ongoing basis to determine when enhancements are required. The College has implemented the following to combat external risk and secure the College network and systems containing Confidential Data:

- Secure user authentication protocols:
- Unique passwords are required for all user accounts; each employee receives an individual user account.
- Server accounts are locked after 3 unsuccessful password attempts.
- Computer access passwords are disabled upon an employee's termination.
- User passwords are stored in an encrypted format; VPN passwords are only accessible by system administrators.
- Secure access control measures:
- Access to specific files or databases containing Confidential Data is limited to those employees who require such access in the normal course of their duties.
- CIT staff perform regular internal network security audits to all server and computer system logs to discover to the extent reasonably feasible possible electronic security breaches, and to monitor the system for possible unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of College data.
- Operating system patches and security updates are installed to all servers on a regular basis.
- Antivirus and anti-malware software is installed and kept updated on all servers and workstations.
- Business office personnel use DESlock encryption to send sensitive encrypted email
- Laptops are encrypted by Windows native BitLocker or ESE DESlock disk encryption

6.9 Physical Access

Physical access across the Hebrew College campus, where restricted, is controlled primarily via HID student, faculty and student access cards. Other restricted access locations are controlled by lock and key. Access cards are configured, activated and deactivated using the CCURE software by CIT. Faculty, staff, and students must take precautions to safeguard access cards and reporting lost or stolen cards

6.9.1 Building Access

Hebrew College is a locked campus. The doors are locked at all times except that the doors are unlocked during approved functions. Entry when the doors are locked requires an access card.

6.9.1 Physical Access to printed records

Access to physical records is limited to those required to have access by job description. PI records are kept under lock and key throughout the building.

6.9.2 Physical Security of Computer and Communications Equipment

All Hebrew College network equipment must be physically secured. Access to server room, telephone-wiring closets, network-switching rooms, and other areas containing confidential information must be physically restricted. Only authorized personnel have keys to access these rooms.

All employees who must keep Confidential Hebrew College information offsite in order to do their work must possess lockable furniture for the proper storage of this information. At the time of separation from Hebrew College, all confidential information must be returned immediately.

7 Employee Training

In compliance with requirements of the WISP, all administrative employees are required to complete the online security training on an annual basis. Any faculty, student or contract employee that has access to PI is also required to complete this yearly training. The training is also strongly recommended for all employees.

Additionally, users who are the victims of a phishing attack will be required to complete this course within 2 weeks after CIT identifies the issue, regardless of whether or not they have already completed the training. If a user fails to complete the training within 2 weeks, his or her remote access to College resources will be disabled. The CIT Team maintains records of all such training through the Spiceworks helpdesk system.

All employees and contractors must attend a cyber security class annually.

8 Reporting Attempted or Actual Breaches of Security

Any incident of possible or actual unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of PI, or of a breach or attempted breach of the information safeguards adopted under this Program, must be reported immediately to the Director of Information Technology. The Director of Information Technology will contact the VP for Finance and Administration and the Chair of the Emergency Management Team - who will convene the team. The Chair is responsible for coordinating the Emergency Management Team and determining appropriate actions in their response to the breach. The Emergency management Team in coordination with the Director of Information Technology, will document all breaches and subsequent responsive actions taken according to the Hebrew College Incident Response Handling Procedures.

9 Enforcement

Any employee or student who willfully accesses, discloses, misuses, alters, destroys, or otherwise compromises Confidential or Restricted data without authorization, or who fails to comply with this Program in any other respect, will be subject to disciplinary action, which may include termination in the case of employees and expulsion in the case of students.

10 Policies cross-referenced

The following Hebrew College policies provide advice and guidance that relates to this Program:

- Hebrew College Acceptable Use of Information Technology Resources

11 Effective date

This Written Information Security Program was implemented December 2020.

The College will review this Program at least annually and reserves the right to change, modify, or otherwise alter this Program at its sole discretion and at any time as it deems circumstances warrant.

12 Historical Data of all Changes to Document

Revision History

Date	Name	Description of Change
7/27/18	Creation	Policy Created
7/30/18	Update	First revision to include appendices, updates on data classification.
10/29/18	Reviewed after feedback from auditor	Made the document more general leaving the detail to the actual policy documentation.
11/4/19	Added Appendix for Wisp Check List	Added the actual Commonwealth of Massachusetts 201 CMR 17.00 COMPLIANCE CHECKLIST
12/11/20	Approved	Approved by the Data Management team
2/11/21	Updates	Updated Documentation information table on page 1 Updated the footer to reflect last revision date Update the wording in 6.9.1 to be more clear Temporarily removed cross referenced documents for further review Fixed typos Fixed date fields that were not updating to reflect last save and revision.

Appendix A. Massachusetts General Law 93I

1.1.1 Overview of Laws

M.G.L. 93H

- Defines Personal Information.
- Requires the state and affected parties be notified in the event of a security breach or unauthorized usage of personal information.

M.G.L. 93I

- Requires that personal information be destroyed in a manner that leaves it unrecoverable.

201 CMR 17.00

- Requires certain steps to verify that third party vendors with access to personal information do not introduce risk.
- Requires limiting the amount of personal information collected.

M.G.L. Ch. 93H defines Personal Information as an individual's name in combination with any of the following:

- Social Security Number
- Driver's License Number
- State Identification Card Number
- Financial Account Number, credit or debit card number

In addition, M.G.L. Ch. 93I includes Biometric Indicators as Personal Information.

Appendix B. Massachusetts State Wisp Check List

CHARLES D. BAKER
GOVERNOR

KARYN E. POLITO
LIEUTENANT GOVERNOR

JAY ASH
SECRETARY OF HOUSING AND ECONOMIC DEVELOPMENT

JOHN C. CHAPMAN
UNDERSECRETARY

COMMONWEALTH OF MASSACHUSETTS

Office of Consumer Affairs and Business Regulation

10 Park Plaza, Suite 5170, Boston, MA 02116

(617) 973-8700 FAX (617) 973-8799 www.mass.gov/consumer

201 CMR 17.00 COMPLIANCE CHECKLIST

The Office of Consumer Affairs and Business Regulation has compiled this checklist to help small businesses in their effort to comply with 201 CMR 17.00**. This Checklist is not a substitute for compliance with 201 CMR 17.00**. Rather, it is designed as a useful tool to aid in the development of a written information security program for a small business or individual that handles "personal information." Each item, presented in question form, highlights a feature of 201 CMR 17.00 that will require proactive attention in order for a plan to be compliant.

The Comprehensive Written Information Security Program (WISP)

- ☐ Do you have a comprehensive, written information security program ("WISP") applicable to all records containing personal information about a resident of the Commonwealth of Massachusetts ("PI")?
- ☐ Does the WISP include administrative, technical, and physical safeguards for PI protection?
- ☐ Have you designated one or more employees to maintain and supervise WISP implementation and performance?
- ☐ Have you identified the paper, electronic and other records, computing systems, and storage media, including laptops and portable devices that contain personal information?
- ☐ Have you chosen, as an alternative, to treat all your records as if they all contained PI?
- ☐ Have you identified and evaluated reasonably foreseeable internal and external risks to paper and electronic records containing PI?
- ☐ Have you evaluated the effectiveness of current safeguards?
- ☐ Does the WISP include regular ongoing employee training, and procedures for monitoring employee compliance?
- ☐ Does the WISP include disciplinary measures for violators?
- ☐ Does the WISP include policies and procedures for when and how records containing PI should be kept, accessed or transported off your business premises?
- ☐ Does the WISP provide for immediately blocking terminated employees, physical and electronic access to PI records (including deactivating their passwords and user names)?
- ☐ Have you taken reasonable steps to select and retain a third-party service provider that is capable of maintaining appropriate security measures consistent with 201 CMR 17.00?

- ☐ Have you required such third-party service provider by contract to implement and maintain such appropriate security measures?
- ☐ Is the amount of PI that you have collected limited to the amount reasonably necessary to accomplish your legitimate business purposes, or to comply with state or federal regulations?
- ☐ Is the length of time that you are storing records containing PI limited to the time reasonably necessary to accomplish your legitimate business purpose or to comply with state or federal regulations?
- ☐ Is access to PI records limited to those persons who have a need to know in connection with your legitimate business purpose, or in order to comply with state or federal regulations?
- ☐ In your WISP, have you specified the manner in which physical access to PI records is to be restricted?
- ☐ Have you stored your records and data containing PI in locked facilities, storage areas or containers?
- ☐ Have you instituted a procedure for regularly monitoring to ensure that the WISP is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of PI; and for upgrading it as necessary?
- ☐ Are your security measures reviewed at least annually, or whenever there is a material change in business practices that may affect the security or integrity of PI records?
- ☐ Do you have in place a procedure for documenting any actions taken in connection with any breach of security; and does that procedure require post-incident review of events and actions taken to improve security?

Additional Requirements for Electronic Records

- ☐ Do you have in place secure authentication protocols that provide for:
    - Control of user IDs and other identifiers?
    - A reasonably secure method of assigning/selecting passwords, or for use of unique identifier technologies (such as biometrics or token devices)?
    - Control of data security passwords such that passwords are kept in a location and/or format that does not compromise the security of the data they protect?
    - Restricting access to PI to active users and active user accounts?
    - Blocking access after multiple unsuccessful attempts to gain access?

- ☐ Do you have secure access control measures that restrict access, on a need-to-know basis, to PI records and files?
- ☐ Do you assign unique identifications plus passwords (which are not vendor supplied default passwords) to each person with computer access; and are those IDs and passwords reasonably designed to maintain the security of those access controls?
- ☐ Do you, to the extent technically feasible, encrypt all PI records and files that are transmitted across public networks, and that are to be transmitted wirelessly?
- ☐ Do you, to the extent technically feasible, encrypt all PI stored on laptops or other portable devices?
- ☐ Do you have monitoring in place to alert you to the occurrence of unauthorized use of or access to PI?
- ☐ On any system that is connected to the Internet, do you have reasonably up-to-date firewall protection for files containing PI; and operating system security patches to maintain the integrity of the PI?
- ☐ Do you have reasonably up-to-date versions of system security agent software (including mal ware protection) and reasonably up-to-date security patches and virus definitions?
- ☐ Do you have in place training for employees on the proper use of your computer security system, and the importance of PI security?

Appendix C. Electronic Communications Privacy Act

The **Electronic Communications Privacy Act of 1986** (**ECPA**) was enacted by the United States Congress to extend government restrictions on wire taps from telephone calls to include transmissions of electronic data by computer (18 U.S.C. § 2510 *et seq.*), added new provisions prohibiting access to stored electronic communications, i.e., the Stored Communications Act (SCA, 18 U.S.C. § 2701 *et seq.*), and added so-called pen trap provisions that permit the tracing of telephone communications (18 U.S.C. § 3121 *et seq.*). ECPA was an amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the Wiretap Statute), which was primarily designed to prevent unauthorized government access to private electronic communications. The ECPA has been amended by the Communications Assistance for Law Enforcement Act (CALEA) of 1994, the USA PATRIOT Act (2001), the USA PATRIOT reauthorization acts (2006), and the FISA Amendments Act (2008).[1]

Appendix D. Omnibus Crime Control and Safe Streets Act of 1968

Employee Privacy

The Act prohibits "employers from listening to the private telephone conversations of employees or disclosing the contents of these conversations."[5][6] Employers can ban personal phone calls and can monitor calls for compliance provided they stop listening as soon as a personal conversation begins.[5][6] Violations carry fines up to $10,000.[5][6] The Electronic Communications Privacy Act of 1986 expanded these protections to electronic and cell phone communication.[5]

Agreement that I have read and will comply with the written information security policy.

All employees who have network access must submit a signed paper copy of this form. Hebrew College Director of Information Technology will not accept modifications to the terms and conditions of this agreement.

_____

Employee's Printed Name

_____

Employee's Department

_____

Employee's Telephone Number

_____

Employee's Physical Address and Mail Location

I, the user, agree to take all reasonable precautions to assure that Hebrew College internal information, or information that has been entrusted to Hebrew College by third parties, such as customers, will not be disclosed to unauthorized persons. At the end of my employment or contract with Hebrew College, I agree to return to Hebrew College all information to which I have had access as a result of my position with Hebrew College. I understand that I am not authorized to use this information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the internal Hebrew College manager who is the designated information owner. I have access to a copy of the Hebrew College Written Information Security Policy (WISP), I have read and understand the WISP, and I understand how it affects my job. As a condition of continued employment at Hebrew College, I agree to abide by the policies and other requirements found in that manual. I understand that non-compliance will be cause for disciplinary action up to and including system privilege revocation, dismissal from Hebrew College. I agree to choose a difficult-to-guess password as described in the Hebrew College Information Security Policies Manual, I agree not to share this password with any other person, and I agree not to write this password down unless it has been transformed in an unrecognizable way. I also agree to promptly report all violations or suspected violations of information security policies to Information Security Director at helpdesk@hebrewcollege.edu. _____