**I. OBJECTIVE**

The objective of Dartmouth College (“Dartmouth”), in the development and implementation of this comprehensive written information security program (“WISP”), is to create effective administrative, technical and physical safeguards for the protection of personal information (“PI”). The WISP sets forth Dartmouth’s procedure for evaluating its electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting PI.

For purposes of this WISP, “PI” means an individual’s first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such individual:

* Social Security number;
* driver's license number or state-issued identification card number; or
* financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to an individual’s financial account.

“PI” shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

**II. PURPOSE**

The purpose of the WISP is to better:

* Ensure the security and confidentiality of PI;
* Protect against any anticipated threats or hazards to the security or integrity of such information; and
* Protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud.

**III. SCOPE**

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

(1) identified reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing PI;

(2) assessed the likelihood and potential damage of these threats, taking into consideration the sensitivity of the PI;

(3) evaluated the sufficiency of existing policies, procedures, information systems, and other safeguards in place to control risks;

(4) designed and implemented a WISP that puts safeguards in place to minimize those risks, consistent with the requirements of the regulations; and

(5) implemented regular monitoring of the effectiveness of those safeguards.

**IV. DATA SECURITY COORDINATOR**

Dartmouth has designated its Chief Information Security Officer to implement, supervise and maintain the WISP. That designated employee (the “Data Security Coordinator”) will be responsible for:

a. Initial implementation of the WISP;

b. Training employees;

c. Regular testing of the WISP’s safeguards;

d. Evaluating the ability of each of Dartmouth’s third party service providers to implement and maintain appropriate security measures for the PI to which Dartmouth has permitted them access, consistent with the regulations; and requiring such third party service providers by contract to implement and maintain appropriate security measures;

e. Reviewing the scope of the security measures in the WISP at least annually, or whenever there is a material change in Dartmouth’s business and/or educational practices that may implicate the security or integrity of records containing PI; and

f. Conducting training for all administration, faculty, employees, students and/or independent contractors, including temporary and contract employees, who have access to PI, on the elements of the WISP.

**V.** **INTERNAL RISKS**

To combat internal risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing PI, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory and are effective immediately:

***Internal Threats***

* Dartmouth shall only collect PI of students, faculty, or employees that is necessary to accomplish Dartmouth’s legitimate need to access said records or necessary to Dartmouth to comply with state or federal regulations.
* Access to records containing PI shall be limited to those persons who are reasonably required to know such information in order to accomplish Dartmouth’s legitimate business and/or educational purpose or to enable Dartmouth to comply with state or federal regulations.
* Access to PI shall be restricted to active users and active user accounts only.
* Any PI stored shall be disposed of when no longer needed for business and/or educational purposes or required by law for storage. Paper or electronic records (including records stored on hard drives or other electronic media) containing PI shall be disposed of only in a manner that complies with the regulations and as follows:
	+ Paper documents containing PI shall be either redacted, burned, pulverized or shredded upon disposal so that PI cannot be practicably read or reconstructed; and
	+ Electronic media and other non-paper media containing PI shall be destroyed or erased upon disposal so that PI cannot be practicably read or reconstructed.
* A copy of this WISP must be distributed to each current Dartmouth employee with access to PI and to each new Dartmouth employee with access to PI at the commencement of their employment.
* All Dartmouth employees with access to PI shall participate in Dartmouth’s training program on the detailed provisions of the WISP. Each such Dartmouth employee shall sign and acknowledge his/her completion of the training program and agreement to abide by the WISP. Immediate retraining of Dartmouth employees shall occur to the extent the Data Security Coordinator determines a need.
* Procedures for Terminated Employees
	+ Terminated employees must return all records containing PI, in any form, that may at the time of such termination be in the former employee’s possession (including all such information stored on laptops or other portable devices or media, and in files, records, work papers, etc.)
	+ A terminated employee’s physical and electronic access to PI must be immediately blocked.
* All persons who fail to comply with this WISP shall be subject to disciplinary measures, irrespective of whether PI was actually accessed or used without authorization.
* All security measures shall be reviewed at least annually, or whenever there is a material change in Dartmouth’s business and/or educational practices that may reasonably implicate the security or integrity of records containing PI. The Data Security Coordinator shall be responsible for this review and shall fully apprise administration of the results of that review and any recommendations for improved security arising out of that review.
* Recordkeeping Protocol
	+ Employees are prohibited from keeping open files containing PI on their desks when they are not at their desks.
	+ At the end of the work day, all files and other records containing PI must be secured in a manner that is consistent with the WISP’s rules for protecting the security of PI.
	+ Any paper files containing PI shall be stored in a locked filing cabinet. Individual files may be assigned to Dartmouth employees on an as-needed basis.
* Access Control Protocol
	+ Access to electronically stored PI shall be electronically limited to those Dartmouth employees authorized to access PI, via a unique log-in ID and confidential password. Vendor/system default log-in ID’s or passwords are not permitted.
	+ All employee computers that have access to PI and have been inactive for a period of time shall require re-log-in. The inactive period permitted is dependent on the system involved.
	+ After multiple unsuccessful log-in attempts by any user ID, that user ID will be blocked from accessing any computer or file stored on any computer until access privileges are reestablished by Computing Services. The threshold for multiple log-in attempts is dependent on the system involved.
* Whenever there is an incident that requires notification under any state breach notification statute or regulation, there shall be an immediate mandatory post-incident review of events and action taken, if any, with a view to determining whether any changes in Dartmouth’s security practices are required to improve the security of PI for which Dartmouth is responsible.

**VI.** **EXTERNAL RISKS**

To combat external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing PI, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory and are effective immediately:

***External Threats***

* Firewall protection, operating system security patches, and all software products shall be reasonably up-to-date and installed on any computer that stores or processes PI.
* All system security software including, anti-virus, anti-malware, and internet security shall be reasonably up-to-date and installed on any computer that stores or processes PI.
* To the extent technically feasible, all PI stored on laptops or other portable devices shall be encrypted, as must all records and files transmitted across public networks or wirelessly, to the extent technically feasible. Encryption here means the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key.
* There shall be secure user authentication protocols in place that:
	+ Control user ID and other identifiers;
	+ Assigns passwords in a manner that conforms to accepted security standards, or applies use of unique identifier technologies; and
	+ Control passwords to ensure that password information is secure.
* PI shall not be removed from Dartmouth’s premises in electronic or written form absent a legitimate business and/or educational need and use of reasonable security measures, as described in this WISP.
* All computer systems shall be monitored for security system failure and unauthorized use or access to PI.

{2512750:1}