Aveda Institute Montana
Information Security Plan

Background

This Information Security Plan ("Plan") describes Aveda Institute's (the "Institute's") safeguards to protect covered data and information. These safeguards are provided to:

- Promote the security and confidentiality of covered data and information;
- Protect against anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or misuse of covered data and information that could result in substantial harm or inconvenience to any student, employee or customer.

This Information Security Plan also provides for mechanisms to:

- Identify and assess the risks that may threaten covered data and information maintained by the Institute;
- Develop written policies and procedures to manage, control and mitigate these risks;
- Implement and review the plan; and
- Adjust this Plan to reflect changes in technology, the sensitivity of covered data and information and internal or external threats to information security.

"Covered data" is defined as educational records, and the personal and financial information of students, prospective students, faculty members, staff members, alumni and customers. When in doubt as to whether a piece of data or information is to be safeguarded as covered data and information, the Institute's employees/ contractors will err on the side that it is covered data and information. It includes data maintained at the Institute as well as centrally stored data, regardless of the media on which they reside. Employees are charged with safeguarding the integrity, accuracy, and confidentiality of covered data and information as part of the condition of employment.

The Institute recognizes that it has both internal and external risks. These risks include, but are not limited to:

- Unauthorized access of covered data and information by someone other than the owner of the covered data and information
- 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 covered data and information by employees
- Unauthorized requests for covered data and information
- Unauthorized access through hardcopy files or reports
- Unauthorized transfer of covered data and information through third parties.

The Institute recognizes that this may not be a complete list of the risks associated with the protection of covered data and information. Because technology growth is not static, new risks are created regularly. Accordingly, the Institute works with information technology vendors to actively monitor for identification of new risks. The Institute has instituted information technology safeguards including the implementation of a firewall to prevent unauthorized access to or from the Institute's network, antivirus software protection, data loss prevention through automatic secure backups, and regular security updates. The Institute also maintains information on log in details of those employees accessing covered data. The Institute believes its current safeguards are reasonable and, in light of the Institute's current risk assessments are sufficient to provide security and confidentiality to covered data and information maintained by the Institute. Additionally, these safeguards protect against currently anticipated threats or hazards to the integrity of such information.

As required by the Student Aid Internet Gateway (SAIG) Enrollment Agreement entered into by the Institute, the Institute must ensure that all Federal Student Aid (FSA) applicant information is protected from access by or disclosure to unauthorized personnel. Under various Federal and state laws and other authorities, including the Higher Education Act of 1965, as amended ("HEA"); the Family Educational Rights and Privacy Act (FERPA); the Privacy Act of 1974, as amended; the Gramm-Leach-Bliley Act; state data breach and privacy laws; and potentially other laws, the Institute may be responsible for losses, fines and penalties (including criminal penalties) caused by data breaches.

The HEA also requires the Institute to maintain appropriate institutional capability for the sound administration of the Title IV programs. Such capability includes satisfactory policies, safeguards, monitoring and management practices related to information security. Further, FERPA generally prohibits institutions from having policies or practices that permit the disclosure of education records or personally identifiable information contained therein without the written consent of the student, unless an exception applies. Any data breach resulting from a failure of an institution to maintain appropriate and reasonable information security policies and safeguards could also constitute a FERPA violation.

To support the expectation and the SAIG requirements described above, the Institute is committed to follow industry standards and best practices in managing information and information systems and in securing covered data, including personally identifiable information. In addition, this Plan is intended to address the requirements of NIST SP 800-171 as set forth on Schedule 1.

Designated Information Security Plan Coordinator

A. Coordinator

Kennedy Payne, the Institute's Assistant Director of Education, serves as the designated Information Security Plan Coordinator as well as the Security Program Officer. All correspondence and inquiries about Institute's Information Security Plan should be directed to Ms. Payne. In the event that Ms. Payne is unavailable, Sandy Schafer serves as the alternate Information Security Plan Coordinator. The coordinators are responsible for the Institute's information security programs and for implementing procedures to minimize risks security risks relating to covered data and information on behalf of the Institute and its students.

B. Correspondence and Inquiries

Correspondence and inquiries regarding this Plan should be directed to the coordinators at:

Information Security Plan Coordinator
Kennedy Payne
901 24th Street West
Billings, MT 59102
Phone: 406-652-2700
Email: kpayne@avedainstitutemontana.com

Alternative Coordinator
Sandy Schafer
901 24th Street West
Billings, MT 59102
Phone: 406-652-2700
Email: sschafer@avedainstitutemontana.com

Student Privacy Provisions & Access to Cumulative Records

The Institute respects each student's right to privacy, and acts in accordance with the Family Educational Rights and Privacy Act (FERPA) of 1974. FERPA provides students certain rights with respect to the student access to and amendment of educational records and governs when the Institute can disclose educational records without student consent. FERPA also provides students with the right to complain to the U.S. Department of Education if the student believes the Institute is not in compliance with the statute and governs when the Institute can disclose directory information about students.

FERPA generally requires that the Institute have the student's written permission to release any information from their records except certain types of "directory information." Certain information, classified as "directory information," is available for public consumption unless the student specifically directs that it be withheld. The student may direct the Institute not to disclose such information. Public directory

information as defined by FERPA includes: student's name, address, telephone number, email address, date and place of birth, program of study, honors and awards, dates of attendance and enrollment status. However, the Institute will notify students about directory information and allow them a reasonable amount of time to request that the school not disclose directory information about them.

Students seeking access to their records should submit a written request that identifies the record or records they wish to inspect to the Assistant Director of Education. The Institute will arrange for access and notify the student of the time and place where the records may be inspected. The Institute may charge a reasonable fee for copies of student records.

In accordance with FERPA, the Institute will disclose information from the academic records of a student to authorized persons, provided the Institute has on file written consent of the student. The form is available from the Assistant Director of Education's office. A student must submit a written consent for each third-party request for information.

Security Provisions

The Aveda Institute Montana Information Security Plan herein is designed to ensure the security, integrity, and confidentiality of covered data, including but not limited to non-public personally identifiable information, protecting it against anticipated threats, and guarding it against unauthorized access or use. Covered under the Plan are administrative, technical, and physical safeguards used in the collection, distribution, processing, protection, storage, use, transmission, handling, or disposal of covered data. The Plan covers actions by both employees of the Institute and outside service providers.

The Institute uses direct personal control or direct supervision to control access to and handling of all covered data when an office is open. Whether the information is stored in paper form or any electronically accessible format, covered data is maintained, stored, transmitted and otherwise handled under the direct personal control of an authorized employee of the Institute.

Covered data is collected, processed, transmitted, distributed and ultimately disposed of with constant attention to its privacy and security. The Institute and its employees will only collect and use covered data that is absolutely necessary. Conversations concerning covered data are held in private. Papers with covered data are mailed via US mail, or private mail carrier. When best practices permit the disposal of non-public information, it is destroyed; paper containing such information is routinely shredded or otherwise destroyed.

Institute employees are required to password-protect electronic files of non-public personally identifiable information when transmitting electronically.

Confidential material is kept secure. Most offices have locked windows and locked doors with restricted access. For those that do not, materials are kept in locked filing cabinets or other locked storage areas. When offices are open, confidential information is kept out of sight from visitors, and computer screens are not visible to visitors. Offices and/or computers are locked when the office will be vacant for an extended length of time.

Key access is limited to authorized Institute employees only, and the Institute's Director of Education governs the distribution of keys. The Institute's Director of Education further ensures the security of offices at the campus after hours.

Credit Card Policy

This Information Security Plan includes the Institute's credit card security requirements as required by the Payment Card Industry Data Security Standard (PCI DSS) Program. The Institute is committed to these security policies to protect information utilized by the school in attaining its business goals. All employees are required to adhere to the policies described within this document.

- It is against Institute policy to store credit card numbers on any document, computer, server, or database. This includes Excel spreadsheets.
- Email is not an approved way to transmit credit card numbers.
- Fax transmittal of cardholder data is permissible only if the receiving fax is located in a secure environment and the credit card number is not visible.
- Paper receipts including covered data or credit card numbers must be destroyed so that account information is unreadable and cannot be reconstructed.
- The Institute will regularly update anti-virus software.
- Employees may not use vendor-supplied defaults for systems passwords and other security parameters.
- Each computer with any sensitive information or access to the administrative network must be password protected.

The PCI requirements apply to all systems that store, process, or transmit cardholder data. Currently, our cardholder environment consists only of standalone terminals. The environment does not include storage of cardholder data on any computer system. Should the Institute implement additional acceptance channels, begin storing, processing, or transmitting cardholder data in electronic format, or otherwise become ineligible to validate compliance under applicable statutory and/or regulatory requirements, it will be the school's responsibility to determine the appropriate compliance criteria and implement additional policies and controls as needed.

Employee Management and Training

All Aveda Institute Montana employees, including part-time and temporary employees, are given specific training by their supervisors about issues of security of sensitive and confidential material used in their respective offices. During employee orientation, new employees will receive training on the importance of confidentiality of student

records, student financial information, and other types of covered data and information, including personal information. Training of new and current employees will include controls and procedure to prevent employees from providing confidential information to an unauthorized individual and how to properly dispose of documents containing sensitive and confidential information. All employees will receive training in the proper use of computer information and passwords. The Security plan officer is responsible for maintaining records on training (names of employees receiving training and dates of training) and is responsible for reviewing and updating training materials as necessary. Employees are held accountable to know that although they have access to non-public information in order to perform their duties for the Institute, they are not permitted to access it for unapproved purposes or disclose it to unauthorized persons. The Employee Handbook, which is provided to all employees, states that violation of security policies could result in termination of employment or legal action, or both.

Outside Service Providers

Third party service providers are required to maintain appropriate safeguards for nonpublic information to which they have access. Contracts with service providers, who within their contracts have access to the Institute's non-public student, prospective student, employee and/or customer information, shall include the following provisions as appropriate:

- Explicit acknowledgment that the contract allows the contract partner access to confidential information;
- Specific definition of the confidential information being provided;
- Stipulation that the confidential information will be held in strict confidence and accessed only for the explicit business purpose of the contract;
- Guarantee from the contract partner that it will ensure compliance with the protective conditions outlined in the contract;
- Guarantee from the contract partner that it will protect the confidential information it accesses according to commercially acceptable standards and no less rigorously than it protects its own customers' confidential information;
- Provision allowing for the return or destruction of all confidential information received by the contract partner upon completion of the contract;
- Stipulation that any violation of the contract's protective conditions amounts to a material breach of contract and entitles the Institute to immediately terminate the contract without penalty;
- Provision allowing auditing of the contract partners' compliance with the contract safeguard requirements;
- Provision ensuring that the contract's protective requirements shall survive any termination agreement.

If the Institute has entered into an arrangement with an outside servicer provider, note that Federal regulation 34 CFR §668.25 includes a provision that the Institute remains liable for any action by its third-party servicers.

Reassessment of Plan

This Plan is reviewed at least annually and adjusted as needed. The Director of Education shall circulate this policy to the advisory board and request a reassessment. The annual review includes identification and assessment of internal and external risks to the security, integrity, and confidentiality of non-public personally identifiable information, including review of outside contractors and their contracts to ensure that proper safeguards are in place.

Information Technology Systems Practices/Policies:

Access to covered data and information via the Institute's computer information system is limited to those employees who have a business reason to know such information. Each employee is assigned a user name and password. Databases containing personal covered data and information, including, but not limited to, accounts, balances, and transactional information, are available only to Institute employees in appropriate departments and positions. Security configuration settings are implemented for IT products that facilitate access covered data. Databases containing personal covered data and information, including but not limited to, accounts, balances, and transactional information, are available only to the Institute employees in appropriate departments and positions. Account and password information is only provided after receipt of documentation from the appropriate supervisor. Network connection for sessions are terminated after a defined period of inactivity. The Institute will take reasonable and appropriate steps consistent with current technological developments to make sure that all covered data and information is secure and to safeguard the integrity of records in storage and transmission. User and system passwords are required to comply with the Institute's password policy described below. When commercially reasonable, encryption technology will be utilized for both storage and transmission. All covered data and information will be maintained on servers that are either behind the Institute's firewall or stored in cloud-based data storage solutions with vendors whose data security systems comply with this Policy. All firewall software and hardware maintained by the Institute will be kept current. Paper documents that contain sensitive or confidential information shall be shredded at time of disposal.

Student Information System – Kennedy Payne, the Institute's Security Program Officer, is responsible for authorizing system access to the School Management and Record Tracking (SMART) student management software system. Each employee's new hire paperwork will indicate whether the employee is authorized to have access to SMART and, if so, the access credentials to be provided. For example, employees in the Institute's student services office will be provided full access to the SMART student profile database (exclusive of user administration). Access for instructors will generally be limited to student grades and attendance records and will exclude access to student personally identifiable information (including but not limited to financial aid information). Each employee's access will be determined by the Security Program Officer and the employee's supervisor in consideration of the employee's job responsibilities.

System privileges are authorized by the Security Program Officer. Staff granted access to institutional data may do so only to conduct Institute business. In this regard, employees must:

- Respect the confidentiality and privacy of individuals whose records they access
- Observe ethical restrictions that apply to the data to which they have access
- Abide by applicable laws or policies with respect to access, use, or disclosure of information

Employees may not:

- Disclose data to others, except as required by their job responsibilities
- Use data for their own personal gain, nor for the gain or profit of others
- Access data to satisfy their personal curiosity

Employees and students who violate this policy are subject to the investigative and disciplinary procedures of the Institute. The Director of Education handles complaints against students as well as complaints against staff and administrators.

Access to information technology systems is granted based on the employee's need to use specific data, as defined by job duties, and subject to appropriate approval. As such, this access cannot be shared, transferred or delegated. Failure to protect these resources may result in disciplinary measures being taken against the employee, up to and including termination. Upon an employee's termination from the Institute, access to the Institute's IT system is terminated.

Reviews: The Security Program Officer is responsible for conducting annual reviews to assess the internal control structure and to verify that that the Institute is in compliance with requirements and applicable state and federal laws.

Employee Information

All aspects of personnel records are confidential. Directory information for employees is public. Directory information may include some or all of the following: name, department, position title, Institute address, Institute phone and email address. Employees may request that this data be classified as confidential. All other employee related data must be vigilantly safeguarded and treated as confidential.

Passwords

Administrative information is protected through the vigilant use of user-defined passwords. Passwords must:

- Include at least one uppercase letter, one lowercase letter, one number, and one symbol or character
- Be eight characters in length, minimum
- Individuals are expected to protect passwords from disclosure. Every individual must have a unique user login.

Disposal of Covered Information
The Institute retains Covered Information for the period of time extending to the time that it has a legitimate business need or legal requirement to hold on to it or for such additional time if targeted disposal isn't feasible because of the way the information is maintained. During all times, Covered Information is maintained in the secure manner as described in this Plan.

Communication to New Employees
The Security Program Officer is responsible for discussing this policy with each employee at the time system privileges are issued. Effective, on-going communication of this security policy along with instruction regarding office procedures is the responsibility of the Institute's Security Program Officer.

Unauthorized Disclosure of Covered Information
Any actual or suspected unauthorized disclosure of covered information must be immediately reported to the Security Program Officer, who in turn shall immediately report such actual or suspected unauthorized disclosure to the Institute's Director of Education.

The Security Program Officer will immediately examine the initial information to confirm a breach has occurred. Once a breach has been validated, the Security Program Officer will serve as an incident manager to coordinate the incident response. The Security Program Officer will begin breach response documentation and reporting process and coordinate the flow of information and manage public message about the breach.

The Security Program Officer shall also assemble an incident response team. This may include representatives from management, information technology, legal, and finance (and possibly HR, for internal incidents) in the incident response team. The team shall immediately determine the status of the breach (on-going, active, or post breach). If the breach is active or on-going, the team shall take action to prevent further data loss by securing and blocking unauthorized access to systems/data and preserve evidence for investigation. All mitigation efforts shall be documented for later analysis. Staff who are informed of the breach shall be advised to keep breach details in confidence until notified otherwise.

If criminal activity is suspected, the Security Program Officer shall notify law enforcement and follow any applicable federal, State, or local legal requirements relating to the notification of law enforcement. The decision to involve outside entities, including law enforcement, should generally be made in consultation with school administration and legal counsel.

The Security Program Officer, in cooperation with the incident response team, shall decide how to investigate the data breach to ensure that the investigative evidence is appropriately handled and preserved. This investigation shall include:

- Identifying all affected data, machines, systems and devices.

- Conducting interviews with key personnel and document facts (if criminal activity is suspected, coordinate these interviews with law enforcement).
- When possible, preserving evidence (backups, images, hardware, etc.) for later forensic examination.
- Locating, obtaining, and preserving (when possible) all written and electronic logs and records applicable to the breach for examination.
- Once investigative activities have been completed, safely storing, recording, and/or destroying (where appropriate) all evidence.
- Considering all alternatives to replacing or clearing compromised resources and machines, including the cost of remediation or rebuilding of the assets to an acceptable security level.

The Security Program Officer will consult with the school's legal counsel to examine any applicable federal, State, and local breach reporting requirements to determine which additional authorities or entities must be notified in order to satisfy compliance requirements. This shall also include a determination of whether notification of affected individuals is appropriate and, if so, when and how to provide such notification

The Security Program Officer and incident report team will collect and review any breach response documentation and analyses reports. They shall:

- Assess the data breach to determine the probable cause(s) and minimize the risk of future occurrence.
- Address and/or mitigate the cause(s) of the data breach.
- Solicit feedback from the responders and any affected entities.
- Review breach response activities and feedback from involved parties to determine response effectiveness.
- Make necessary modifications to the school's response strategy to improve the response process.
- Enhance and modify the school's information security and training programs, which includes developing countermeasures to mitigate and remediate pervious breaches; lessons learned must be integrated so that past breaches do not reoccur.

The Institute's SAIG Agreement includes a provision that in the event of an unauthorized disclosure or an ***actual or suspected*** breach of applicant information or other sensitive information (such as personally identifiable information) the Institute must ***immediately*** notify the U.S. Department of Education Federal Student Aid at CPSSAIG@ed.gov. The Security Program Officer shall notify the Institute's Director of Education that an unauthorized disclosure or suspected breach of applicant information or other sensitive information has occurred. The Director of Education, working with the Security Program Officer, shall then submit the required notification to FSA as required under the SAIG Agreement.

EMPLOYEE GUIDELINES FOR SECURING COVERED DATA AND INFORMATION:

"Covered Data" is defined as educational records, and the personal and financial information of students, prospective students, faculty members, staff members, alumni and customers. When in doubt as to whether a piece of data or information is to be safeguarded as covered data and information, Institute employees/contractors will err on the side that it is covered data and information. Covered data and information includes both paper and electronic records. Examples of personal and financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories, and social security numbers.

Every Institute employee who has access to covered data and information is responsible for:

1. Maintaining physical security by locking rooms and/or file cabinets where covered data and information is stored. Ensuring windows are locked and using safes when practicable for especially sensitive covered data and information.

2. Maintaining adequate key control and limiting access to sensitive areas to those individuals with a "need to know" in order to perform their job.

3. Using passwords to access automated systems that process covered data and information. Also requiring the use of "strong" passwords (e.g. at least 8 characters, and not easily guessable). Also requiring the safeguarding of passwords (e.g. do not leave passwords written down in easy view of others in the vicinity of an employee's work area).

4. Using firewalls and encrypting covered data and information when appropriate and feasible.

5. Referring calls and mail requesting covered data and information to those individuals who have been trained in safeguarding covered data and information for these types of requests.

6. Shredding and erasing customer information when no longer needed in accordance with Institute policy.
7. Taking reasonable efforts to limit the view of computer screens and other mediums (e.g. paper) displaying covered data and information to only those employees who have a "need to know" in order to perform their job.

8. Erasing covered data and information from computer screens when it is no longer in use. And never leave your desk area with covered data and information still displayed on a computer screen or on some other medium (e.g. paper) on the desk in clear site of a casual passerby.

9. Encouraging employees to report suspicious activity to supervisors and/or the Director of Education, as appropriate.
10. Encouraging password-activated screen savers and using them when an employee is away from his/her desk.

11. Taking reasonable steps to ensure that all future contracts are with service providers that are capable of maintaining appropriate safeguards for the covered data and information at issue.

Disciplinary measures (including job termination) may be taken against any employee who intentionally, or through gross negligence, violates any of the above guidelines.

Statement of Understanding

Please read the following information and sign this form at the bottom indicating your agreement to comply with students' privacy rights as protected by the Family Educational Rights and Privacy Act (FERPA) and the Gramm- Leach-Bliley Act (GLBA). Return this form to the Director of Education.

Family Education Rights and Privacy Act ("FERPA")
The purpose of the Family Educational Rights and Privacy Act is to afford certain rights to students concerning their education records, and one of these FERPA rights is to have some control over the disclosure of personally identifiable information from their records. Personally identifiable information contained in education records may not be disclosed without the student's written consent except to school officials whom the Institute has determined have a legitimate educational interest.

Legitimate Educational Interest means the demonstrated need to know by those officials of an institution who act in the student's educational interest, including faculty, administration, professional staff and other designated staff.

Information that cannot be disclosed without a student's written consent:

- Name of the student in combination with any of the following items,
- Student's parents or other family member,
- Student or family address,
- Student's Social Security number, Personal Identification Number (PIN) or other identifying number,
- Student's schedule,
- List of personal characteristics (such as gender, race, ethnicity or religion),
- Grading or attendance information
- Other information that could make the student's identity easily traceable.

Gramm-Leach-Bliley Act ("GLBA")
The purpose of the GLBA is to afford certain rights to students, faculty members, staff members and alumni concerning their personal and financial information. A focus of GLBA is to control the disclosure of personally identifiable information maintained by the Institute in the necessary course of business. Institutions may not disclose personally identifiable information, without the student's, faculty member's, staff member's or alumni's written consent except to school officials whom the institution has determined to have a legitimate interest.

ACCEPTANCE OF RESPONSIBILITY

I understand that the Aveda Institute Montana maintains personally identifiable information for students, prospective students, faculty members, staff members, alumni and customers, disclosure of which is prohibited by the Family Education Rights and Privacy Act and the Gramm-Leach-Bliley Act. I acknowledge that I fully understand that the intentional disclosure by me of this information to any unauthorized person could subject me to criminal and civil penalties imposed by law. I further acknowledge that such willful or unauthorized disclosure of student information also violates Institute policies and could constitute just cause for disciplinary action including termination of my employment regardless of whether criminal or civil penalties are imposed.

I also understand that I am liable for any unauthorized use of, or access to, information protected by FERPA and GLBA by any other person accessing information via my password due to my own negligence or carelessness.

_____

Name

_____

Signature Date

REQUIREMENT	Institute Policy
Access Control	See Security Provisions, IT Systems Practices/Policies
Awareness and Training	See Employee Management and Training; Communications to New Employees
Audit and Accountability	Outside Audit; Also see Security Provisions
Configuration Management	See Information Technology Systems Practices/Policies
Basic Security Requirements	See Information Technology Systems Practices/Policies, Security Provisions, Passwords
Incident Response	See Unauthorized Disclosure of Covered Information
Maintenance	See Reassessment of Plan
Media Protection	See Unauthorized Disclosure of Covered Information
Personnel Security	See Security Provisions; Employee Management and Training; Outside Service Providers, Student information System
Physical Protection	See Security Provisions, Information Technology Systems Practices/Policies; Passwords
Risk Assessment	See Reassessment of Plan,
Security Assessment	See Reassessment of Plan, Designated Information Security plan coordinator
System & Communication Protection	See Security Provisions, Information Technology Systems Practices/Policies
System & information Integrity	See Security Provisions, Information Technology Systems Practices/Policies

SCHEDULE 1 – NIST SECURITY CONTROLS