PREMIERE AESTHETICS INSTITUTE

Information Security Plan

Contents

Introduction

This Information Security Plan encompasses all aspects of security surrounding covered data and information and must be distributed to all company employees. All company employees must read this document in its entirety and sign the form confirming they have read and fully understand this policy. This Plan is reviewed at least annually and adjusted as needed. 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.

This Information Security Plan describes Premier Aesthetics Institute's ("PAI'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 Premier Aesthetics 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, Premier Aesthetics Institute employees/contractors will err on the side that it is covered data and information. It includes data maintained at PAI 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.

Premier Aesthetics 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

Premier Aesthetics 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, PAI works with information technology vendors to actively

monitor for identification of new risks. See Appendix C for a list of service providers. PAI has instituted information technology safeguards including the implementation of a firewall to prevent unauthorized access to or from PAI's network, antivirus software protection, data loss prevention through automatic secure backups, and regular security updates. PAI believes its current safeguards are reasonable and, in light of PAI's current risk assessments are sufficient to provide security and confidentiality to covered data and information maintained by PAI. 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 PAI, PAI 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, PAI may be responsible for losses, fines and penalties (including criminal penalties) caused by data breaches.

The HEA also requires PAI 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, PAI 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.

Employees handling sensitive covered data should ensure:

- Handle Company and covered data in a manner that fits with their sensitivity and classification;
- Limit personal use of PAI information and telecommunication systems and ensure it doesn't interfere with your job performance;
- PAI reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose;
- Do not use e-mail, internet and other Company resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal;
- Do not disclose personnel information unless authorized;
- Protect sensitive covered data information;
- Keep passwords and accounts secure;
- Enable the use of multi-factor authentication, where available, to ensure authorized access PAI information systems and protected covered information;
- Request approval from management prior to establishing any new software or hardware, third party connections, etc.;

- Do not install unauthorized software or hardware, including modems and wireless access unless you have explicit management approval;
- Always leave desks clear of sensitive covered data and lock computer screens when unattended;
- Information security incidents must be reported, without delay, to the Information Security Plan Coordinator.

We each have a responsibility for ensuring our company's systems and data are protected from unauthorised access and improper use. If you are unclear about any of the policies detailed herein you should seek advice and guidance from the Information Security Plan Coordinator and/or your School Director.

1. Designated Information Security Plan Coordinator

John Smith serves as the designated Information Security Plan Coordinator as well as the Security Plan Coordinator. All correspondence and inquiries about PAI's Information Security Plan should be directed to Mr. Smith. In the event that Mr. Smith is unavailable, Kayleen Quiros serves as the alternate Information Security Plan Coordinator. In addition to the designated Security Plan Coordinators, Mr. Smith is responsible for overseeing information technology at PAI and is in charge of information and security testing procedures. The coordinators are responsible for PAI's information security programs and for implementing procedures to minimize risks security risks relating to covered data and information on behalf of PAI and its students.

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

Information Security Plan Coordinator
John Smith
1133 NW Wall St., Suite 102
Bend, OR 97703
Email: mailto:John@premiereaestheticsinstitute.com
Phone: 541-797-6578

Alternative Coordinator
Kayleen Quiros
1133 NW Wall St., Suite 102
Bend, OR 97703
Email: kayleen@premiereaestheticsinstitute.com
Phone:541-797-6578

2. Network Security

A high-level network diagram of the network is maintained and reviewed on a yearly basis. The network diagram provides a high-level overview of the covered data environment (CDE), which at a minimum shows the connections in and out of the CDE. Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable should also be illustrated.

3. Acceptable Use Policy

Management's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to PAI established culture of openness, trust and integrity. Management is committed to protecting the employees, partners and the Company from illegal or damaging actions, either knowingly or unknowingly by individuals. PAI will maintain an approved list of technologies and devices and personnel with access to such devices as detailed in Appendix B.

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
- Employees should take all necessary steps to prevent unauthorized access to confidential data which includes covered data.
- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
- All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature.
- All POS and PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered.
- The List of Devices in Appendix B will be regularly updated when devices are modified, added or decommissioned. A stocktake of devices will be regularly performed and devices inspected to identify any potential tampering or substitution of devices.
- Users should be trained in the ability to identify any suspicious behaviour where any tampering or substitution may be performed. Any suspicious behaviour will be reported accordingly.
- Information contained on portable computers is especially vulnerable, special care should be exercised.
- Postings by employees from a Company email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of PAI, unless posting is in the course of business duties.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4. Protect Stored Data

The Premiere Aesthetics Institute 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 PAI and outside service providers.

PAI 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 PAI.

Covered data is collected, processed, transmitted, distributed and ultimately disposed of with constant attention to its privacy and security. PAI 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.

PAI 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 PAI employees only, and the Director governs the distribution of keys. The Director further ensures the security of offices at the campus after hours.

5. Physical Security

Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorized individuals from obtaining sensitive data.

- Media is defined as any printed or handwritten paper, received faxes, floppy disks, back-up tapes, computer hard drive, etc.
- Media containing sensitive covered information must be handled and distributed in a secure manner by trusted individuals.
- Visitors must always be escorted by a trusted employee when in areas that hold sensitive information.
- Procedures must be in place to help all personnel easily distinguish between employees and visitors, especially in areas where covered data is accessible. “Employee” refers to full-time and part-time employees, temporary employees and personnel, and consultants who are “resident” on PAI sites. A “visitor” is defined as a vendor, guest of an employee, service personnel, or anyone who needs to physically enter the premises for a short duration, usually not more than one day.
- POS devices surfaces are periodically inspected to detect tampering or substitution.
- Personnel using the devices should be trained and aware of handling the POS devices
- Personnel using the devices should verify the identity of any third party personnel claiming to repair or run maintenance tasks on the devices, install new devices or replace devices.
- Personnel using the devices should be trained to report suspicious behaviour and indications of tampering of the devices to the appropriate personnel.
- Strict control is maintained over the external or internal distribution of any media containing covered data and has to be approved by management
- Strict control is maintained over the storage and accessibility of media
- All computer that store sensitive covered data must have a password protected screensaver enabled to prevent unauthorised use.

6. Credit Card Policy

This Information Security Plan includes PAI’s credit card security requirements as required by the Payment Card Industry Data Security Standard (PCI DSS) Program. PAI 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 PAI 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.
- PAI 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 PAI 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.

7. Protect Data in Transit

All sensitive covered data must be protected securely if it is to be transported physically or electronically.

- Covered data must never be sent over the internet via email, instant chat or any other end user technologies.
- If there is a business justification to send covered data via email or by any other mode then it should be done after authorization and by using a strong encryption mechanism (i.e. – AES encryption, PGP encryption, IPSEC, etc.).
- The transportation of media containing sensitive covered data to another location must be authorized by management. Only secure courier services may be used for the transportation of such media. The status of the shipment should be monitored until it has been delivered to its new location.

8. Disposal of Stored Data

- PAI retains covered data 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 data is maintained in the secure manner as described in this Plan.
- All data must be securely disposed of when no longer required by PAI, regardless of the media or application type on which it is stored.
- An automatic process must exist to permanently delete on-line data, when no longer required.
- All hard copies of covered data must be manually destroyed when no longer required for valid and justified business reasons.

- PAI will have procedures for the destruction of hardcopy (paper) materials. These will require that all hardcopy materials are crosscut shredded, incinerated or pulped so they cannot be reconstructed.
- PAI will have documented procedures for the destruction of electronic media. These will require:
    - All covered data on electronic media must be rendered unrecoverable when deleted;
    - If secure wipe programs are used, the process must define the industry accepted standards followed for secure deletion.

9. Security Awareness and Procedures

The policies and procedures outlined below must be incorporated into company practice to maintain a high level of security awareness. The protection of sensitive data demands regular training of all employees and contractors.

- Review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into day-to-day company practice.
- 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
- Distribute this security policy document to all company employees to read. It is required that all employees confirm that they understand the content of this security policy document by signing an acknowledgement form (see Appendix A).
- All employees that handle sensitive information will undergo background checks (such as criminal and credit record checks, within the limits of the local law) before they commence their employment with the Company.
- Company security policies must be reviewed annually and updated as needed.

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

11. Unauthorized Disclosure Incident Response Plan

Any actual or suspected unauthorized disclosure of covered information must be immediately reported to the Security Plan Coordinator, who in turn shall immediately report such actual or suspected unauthorized disclosure to PAI's President.

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

The Security Plan Coordinator 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 Plan Coordinator 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 Plan Coordinator, 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 Plan Coordinator and/or President of Premiere Aesthetics Institute 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 Plan Coordinator 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.

PAI'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) PAI must ***immediately*** notify the U.S. Department of Education Federal Student Aid at CPSSAIG@ed.gov. The Security Plan Coordinator shall notify PAI's President that an unauthorized disclosure or suspected breach of applicant information or other sensitive information has occurred. The President, working with the Security Plan Coordinator, shall then submit the required notification to FSA as required under the SAIG Agreement.

The following information should be included in any such notice:

- Date of Breach (Suspected or Known)
- Impact of Breach (# of records, etc.)
- Method of Breach (Hack, accidental disclosure, etc.)
- Information Security Program Point of Contact Email and Phone details
- Remediation Status (complete, in-process- with detail, etc.)
- Next steps (as needed)

12. User Access Management

- Access to PAI is controlled through a formal user registration process beginning with a formal notification from HR or the School Director .
- Each user is identified by a unique user ID so that users can be linked to and made responsible for their actions. The use of group IDs is only permitted where they are suitable for the work carried out.
- There is a standard level of access; other services can be accessed when specifically authorized by HR/line management.
- The job function of the user decides the level of access the employee has to covered data
- A request for service must be made in writing (email or hard copy) by the newcomer's line manager or by HR. The request is free format, but must state:

Name of person making request;
Job title of the newcomers and
workgroup; Start date;
Services required (default services are: MS Outlook, MS Office and Internet access).

- Each user will be given a copy of their new user form to provide a written statement of their access rights, signed by an IT representative after their induction procedure. The user signs the form indicating that they understand the conditions of access.
- Access to all PAI systems is provided by IT and can only be started after proper procedures are completed.
- As soon as an individual leaves PAI employment, all his/her system logons must be immediately revoked.
- As part of the employee termination process HR (or line managers in the case of contractors) will inform IT operations of all leavers and their date of leaving.

Student Information System: PAI's Security Plan Coordinator is responsible for authorizing system access to _____. Each employee's new hire paperwork will indicate whether the employee is authorized to have access to _____ and, if so, the access credentials to be provided. For example, employees in PAI's student services office will be provided full access to the _____ 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 Plan Coordinator and the employee's supervisor in consideration of the employee's job responsibilities.

System privileges are authorized by the Security Plan Coordinator. Staff granted access to institutional data may do so only to conduct PAI 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 PAI. The Director 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 PAI, access to PAI's IT system is terminated.

13. Access Control Policy

- Access Control systems are in place to protect the interests of all users of PAI computer systems by providing a safe, secure and readily accessible environment in which to work.
- PAI will provide all employees and other users with the information they need to carry out their responsibilities in an as effective and efficient manner as possible.
- Generic or group IDs shall not normally be permitted, but may be granted under exceptional circumstances if sufficient other controls on access are in place.
- The allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted and controlled, and authorization provided jointly by the system owner and IT Services. Technical teams shall guard against issuing privilege rights to entire teams to prevent loss of confidentiality.
- Access rights will be accorded following the principles of least privilege and need to know.
- Every user should attempt to maintain the security of data at its classified level even if technical security mechanisms fail or are absent.
- Users electing to place information on digital media or storage devices or maintaining a separate database must only do so where such an action is in accord with the data's classification.
- Users are obligated to report instances of non-compliance to the PAI Information Security Plan Coordinator.
- Access to PAI IT resources and services will be given through the provision of a unique Active Directory account and complex password.
- No access to any PAI IT resources and services will be provided without prior authentication and authorization of a user's PAI Windows Active Directory account.
- Password issuing, strength requirements, changing and control will be managed through formal processes. Password length, complexity and expiration times will be controlled through Windows Active Directory Group Policy Objects.
- Access to Confidential, Restricted and Protected information will be limited to authorised persons whose job responsibilities require it, as determined by the data owner or their designated representative. Requests for access permission to be granted, changed or revoked must be made in writing.
- Users are expected to become familiar with and abide by PAI policies, standards and guidelines for appropriate and acceptable usage of the networks and systems.
- Access for remote users shall be subject to authorization by IT Services and be provided in accordance with the Remote Access Policy and the Information Security Policy. No uncontrolled external access shall be permitted to any network device or networked system.
- Access control methods include logon access rights, Windows share and NTFS permissions, user account privileges, server and workstation access rights, firewall permissions, IIS intranet/extranet authentication rights, SQL database rights, isolated networks and other methods as necessary.
- A formal process shall be conducted at regular intervals by system owners and data owners in conjunction with IT Services to review users' access rights. The review shall be logged and IT Services shall sign off the review to give authority for users' continued access rights.

14. Reassessment of Plan

This Plan is reviewed at least annually and adjusted as needed. The School Director shall circulate this policy to PAI's 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.

The Security Plan Coordinator is responsible for conducting annual reviews to assess the internal control structure and to verify that that PAI is in compliance with requirements and applicable state and federal laws. They are also responsible for periodically reviewing the data retention procedures to minimize unnecessary retention of data. The Security Plan Coordinator will evaluate and adjust the information security program in light of results of the required testing and monitoring. Any material changes in its operation, results from risk assessment, or any other circumstance that may have a material impact on the information security program will be reviewed and evaluated.

Appendix A – Agreement to Comply Form – Agreement to Comply With Information Security Policies

_____

Employee Name (printed)

_____

Department

I agree to take all reasonable precautions to assure that company internal information, or information that has been entrusted to the company by third parties such as students and customers, will not be disclosed to unauthorised persons. At the end of my employment or contract with the company, I agree to return all information to which I have had access as a result of my position. I understand that I am not authorised to use sensitive 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 manager who is the designated information owner.

I have access to a copy of the Information Security Plan, I have read and understand these policies, and I understand how it impacts my job. As a condition of continued employment, I agree to abide by the policies and other requirements found in the company security policy. I understand that non-compliance will be cause for disciplinary action up to and including dismissal, and perhaps criminal and/or civil penalties.

I also agree to promptly report all violations or suspected violations of information security policies to the Information Security Plan Coordinator.

_____

Employee Signature

_____

Appendix B – List of Devices

Oregon:

Asset/Device Name	Description	Owner/Approved User	Location
Front Desk Computer	POS	Maya Deck, all instructors and admin staff	Front Desk
Computer	Instructor/Staff	All Staff	Instructor Office
Laptop	Admin	Kaycee Millington	Admin Office
Laptop	Admin	Kayleen Quiros	Financial Aid Office
Laptop	Admin	Maya Deck	Front Desk
Laptop	Instructor/Staff	All Instructors/Staff	Instructor Office
Chrome Book	Instructors	All Instructors	Classroom B

Idaho:

Asset/Device Name	Description	Owner/Approved User	Location
Front Desk Computer	POS/Staff	Catherine Velasquez, all instructors/staff	Front Desk
Computer	Instructor	All instructors	Classroom 1
Computer	Instructor	All instructors	Classroom 2
Computer	Instructor	All instructors	Classroom 3
Laptop	Student Laptop – for Genesis timeclock & portal access and viewing spa schedule daily	All instructors, staff, students	Dispense area
Computer	Admin	Florentina Badiola/others with prior approval	Financial Office
Computer	Admin	Whitney Barnett/others with prior approval	Assistant Director Office
Computer	Admin	Sharron Prussner/others with prior approval	Director Office
Computer	Public use computer	All instructors and staff without prior approval, all students with prior approval ONLY	Admin Office

Appendix C - List of Service Providers

Name of Service Provider	Contact Details	Services Provided	PCI DSS Compliant	PCI DSS Validation Date
Sysnet	Gopi balachenna +35314951300 balachenna.gopi@sysnetgs. com The Herbert Building Carrickmines Dublin 18 Republic Of Ireland	PCI compliance Remote access software POS software	Yes	04/01/2024

SCHEDULE 1 – NIST

REQUIREMENT	Institute Policy
Access Control	See Physical Security, User Management, Access Control Policy
Awareness and Training	See Security Awareness and Procedures
Audit and Accountability	See Reassessment of Plan, Outside Service Providers
Configuration Management	See Network Security, User Access Management, See also Introduction
Basic Security Requirements	See Acceptable Use Policy, Physical Security, Protect Date in Transit, Credit Card Policy
Incident Response	See Unauthorized Disclosure of Covered Information
Maintenance	See Reassessment of Plan
Media Protection	See Unauthorized Disclosure Incident Response Plan
Personnel Security	See Acceptable Use Policy, Security Awareness and Procedures
Physical Protection	See Physical Security
Risk Assessment	See Reassessment of Plan,
Security Assessment	See Reassessment of Plan, Designated Information Security Plan Coordinator
System & Communication Protection	See Network Security, Acceptable Use Policy, Protect Data in Transit, Outside Service Providers
System & information Integrity	See Network Security, Acceptable Use Policy, Protect Data in Transit