THE SALON PROFESSIONAL
SCHOOL OF COSMETOLOGY

Data privacy, Cyber Incident & Information Security Response Plan

Overview
In accordance to the Department of Education implementing regulations at 34 C.F.R., Standards for Safeguarding Customer Information, 16 C.F.R. Part 314, issued by the Federal Trade Commission (FTC), compliance with the Family Educational Rights and Privacy Act (FERPA), as required by the Gramm-Leach-Bliley Act (GLBA) Act, P.L. 106-102, and upon signing a Program Participation Agreement (PPA) that requires financial institutions to explain their information-sharing practices to their customers and to safeguard sensitive data. Colleges participating in the Federal Student Aid (FSA) programs are subject to the information security requirements established by the FTC for financial institutions. DDBS is responsible for complying with the limitations on the disclosure of PII in students' education records under FERPA and is subject to Sections 501 and 505 (b) (2) of the GLB Act.

Financial Services Modernization Act of 1999 (Public Law 106-102, 113 Statue 1338) also known as the GLB Act regulates the protection, collection, and disclosure of consumers nonpublic personal information or personally identifiable information (PII) by financial institutions.

As a financial institution covered under these information security requirements, The Salon Professional School of Cosmetology (SPSC) has developed, implemented, and maintains a comprehensive data and information security program that is designed to create and implement the following: the written incident response, safeguards to control identified risk, monitor and test regularly/daily the effectiveness of our safeguards, train staff, and monitor our service providers by keeping this information security program current. SPSC has annual risk/ technology assessments provided by Electronic Brain Solution which includes a perform control analysis, assess risk analysis, recommended control measures, and a threat vulnerability statement. SPSC has qualified staff members that oversee, implement, and report to our boards annually any changes, deletions, additions, and suggestions for this program.

Designated Qualified Employees & Personnel Responsible
Kanika Free-Director of Operations

Third-Party Contractual IT Company
Doug Pettigrew -Electronic Brain Solutions
CNA Insurance

Plan Evaluation, Revision, and Training
The Data Privacy, Cyber Incident & Information Security Response Plan is in the Title IV Manuel in hard copy print throughout the school and on digital print on the school website www.thesalonpro.org. This plan is reviewed annually by school committees, and employees. Training for this plan is conducted annually with the personnel responsible for this plan and the third-party contractor who is over all our IT on-site and off-site.

Information Security Plan

This Information Security Plan ("Plan") describes safeguards implemented by DDBS to protect covered data and information in compliance with the FTC's Safeguards Rule promulgated under the Gramm Leach Bliley Act (GLBA). With the use of the following updated firewall configuration, protection, and security software called Huntress, Webroot, Canari, RMM Monitoring, and Pen Testing Scanning. These safeguards are provided to:
• Ensure the security and confidentiality of covered data, student, and information.
• Protect against anticipated threats or hazards to the security or integrity of such information; and
• Protect against unauthorized access to or use of covered data and information that could result in substantial harm or inconvenience to any customer.

Information Security Program
SPSC has developed written policies and procedures to manage control information such as identity and assess the risks that may threaten covered data and information maintained by SPSC. Directories have been created and controlled to allow for the sharing of data in one centralized controlled location. There are adjustments for the future of this program which includes annual and daily meetings and discussions around technology with Staff, Board Members, and IT Contractors which will allow DDBS to reflect on any changes in technology, the sensitivity of covered data/information, and internal or external threats to information security.

Risk Management &Compliance Assessment of Risks to Student/Customer Information
Risk assessments are conducted to identify, quantify, prioritize, and manage risks. Controls, which are applicable to each situation, have been applied to avoid violations of any legal obligation (e.g., statutory, regulatory, or contractual) which is also assessed through Electronic Brain Solutions (EBS). SPSC recognizes that it is exposed to both internal and external risks, including but not limited to the following:

Unauthorized Access: For unauthorized access of covered data and information by someone other than the owner of the covered data and information access control is done by specific sharing with only one person having access to specific data. In addition, SPSC has implemented a policy for risk management & compliance by locking doors, locking computer screens when not in use and not leaving data on screen when not in use, and the use of strong computer passwords. This plan will assist with making sure that data/information is not compromised as result of system access by any unauthorized person.

Interception of Data: The business center at DDBS is responsible for the set-up and management of all email systems through Microsoft. Every message that is sent from the Microsoft account is encrypted. Employees do not use Gmail accounts to send anything with PII. Offsite data backup is encrypted at transit and at rest.

Privacy Settings: The privacy settings on each device can be changed to limit the amount of personal data shared.

Data Back-up
Western Digital Backup is used along with an image backup to the cloud to ensure that data/information is protected offsite with encryption. It is also used for detecting and remediating errors in the system, corruption of data, unauthorized access of covered data and information, unauthorized request for covered data and information/pretext calling which is followed by DDBS policy and procedure that states that no one will be allowed access to PII of another person, unauthorized access through hardcopy files/reports(files are kept in a fire proof locked cabinet in the padlocked data room) and unauthorized transfer of covered data and information

through third party(third parties are vetted and not allowed access to data without an escort of SPSC personnel).

Recognizing that this may not represent a complete list of the risks associated with the protection of covered data and information, and that new risks are created regularly, the SPSC Information Security Program Coordinator along with the third-party contractor Electronic Brain Solutions, will actively participate and monitor appropriate cybersecurity advisory groups for identification of risks. There is also an annual 3rd party penetration testing and remediation assessment that is conducted.

Current safeguards are implemented, monitored, and maintained by the SPSC Information Security Program Coordinator and Electronic Brain Solution (third-party contractor) are reasonable, and considering current risk assessments are sufficient to provide security and confidentiality to covered data and information maintained by the school. Additionally, these safeguards reasonably protect against currently anticipated threats or hazards to the integrity of such information.

Personnel Security Policy and Procedure
References and/or background checks (as appropriate, depending on position) of new employees working in areas that regularly work with covered data and information, financials, and financial aid are checked. DDBS has contractual agreements in place that target keeping client information secure.

Training & Awareness Policy and Procedure
Employees are trained annually to understand this plan and about all changes and revisions to this plan. Employees are taught what is acceptable regarding client data which allows staff to become educated on the secure use of all applications and technology solutions During employee orientation, each new employee in these departments receives proper training on the importance of confidentiality of student hard-copy and digital records, user-groups, student financial information, and all other covered data and information. Each new employee is also trained in the proper use of computer information and passwords. Training includes controls and procedures to prevent employees from providing confidential information to an unauthorized individual, as well as how to properly dispose of documents that contain covered data and information. These training efforts should help minimize risk and safeguard covered data and information. Refresher training is required on an annual basis.

Physical Security Plan/ Policy
SPSC has addressed the physical security of covered data and information that will allow unauthorized parties the inability to access sensitive data by limiting access to only those employees who have a legitimate business reason to handle such information. For example, financial aid applications, income and credit histories, accounts, balances, and transactional information are available only to SPSC employees with an appropriate business need for such information. Furthermore, each department is responsible for maintaining covered data and information and is instructed to take steps to protect the information from destruction, loss, or damage due to environmental hazards such as fire and water damage or technical failures. This Plan/Policy has been implemented, this plan is implemented for permitting and enabling physical access to alternate authorized individuals (e.g., in the event primary authorized individuals are sick or not available).

Information Systems Network Security Plan/Policy
Access to covered data and information via SPSC computer information system is limited to those employees and faculty who have a legitimate business reason to access such information. SPSC has policies and procedures in place including but not limited to access

controls list for any data stored on the server to complement the physical and technical safeguards to provide security to SPSC information systems. Social security numbers are considered protected information under both GLBA and the Family Educational Rights and Privacy Act (FERPA). The following are existing controls:

• Authorized individuals only.
• Workstations with passwords.
• Information sent electronically is encrypted and sent by authorized individuals only.
• Vulnerabilities on both network and systems are constantly monitored and addressed.
• All systems must be managed on a managed services platform to ensure systems are patched when needed.
• Unauthorized access to third parties is not permitted.

Logical Access- Processes are in place to ensure unauthorized access to systems does not take place, users setup using permissions and groups based on job function by doing the following:

• All users must have unique ID" s not only for windows but for 3rd party software as well.
• Email's systems have unique user ID?'s/Passwords in place.
• User rights must be adjusted as needed for employees' current job function.

Operations Management- Operating systems are established to protect documents, computer media, tapes, removeable media, disks, input/output data and system documentation to protect sensitive information from unauthorized disclosure, modification, removal, and destruction by doing the following:

• All sensitive data is handled appropriately by the authorized person.
• Equipment containing data that has been decommissioned or repaired must have any data wiped to DOD
  standards provided the hardware contains any data.
• IT providers will test as needed at their facility.
• Employees will have other employees with different job functions check and double check that data has been entered correctly and is not mistakenly modified.
• Any changes must be discussed with the designated employee(s) that are trained in how to appropriately use equipment/software that was modified to prevent errors and/or risks.

Management of System Failures

SPSC Information Security Program Coordinator has developed procedures to detect any actual or attempted attacks on SPSC systems and has detailed instructions for responding to an actual or attempted unauthorized access to covered data and information. In the event of a system failure The Program Coordinator/Contractual IT Company must first discover the cause of failure (If the failure was due to corrupt files or a hardware failure, addressing/fixing the issue and then restoring from backup), if the cause of the failure is determined to be a third party attack or something malicious, each machine effected should be disconnected from the network but kept running. It is important to contact the cybersecurity insurance provider first for guidance as to how to proceed within the parameters of policy.

Oversight of Service Providers

Electronic Brain Solutions and SPSC will oversee the oversight of service providers by the requirements of the GLBA. SPSC has taken reasonable steps to select and retain service providers who maintain appropriate safeguards for covered data and information. This Information Security Program ensures that such steps are taken by contractually requiring

service providers to implement and maintain such safeguards.

Procedure for Reporting Security Breaches to Students and the Department
The Department considers any breach in the security of student records and information to be a demonstration of a potential lack of administrative capability. Schools' SAIG Agreements include a provision that schools must notify the Department at CPSSAIG@ed.gov the same day of actual breaches as well as suspected breaches of the security of student records and information, and ED strongly encourages schools to notify their students of the breach at the same time.

In their reports to the Department, schools should include the following:
• 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)
• Next steps (as needed)

If you cannot email, contact the Departments security operations center (EDSOC) at 202-245-6550 to report data listed above. EDSOC operates 24 hours a day, seven days per week.

Procedures to Maintain Compliance with the GLB Act Re: Personally Identifiable Information (PII)
1.   All records containing PII are stored and maintained in a secure location.
• Paper records and files are always stored in a locked fireproof cabinet in a locked room that is locked when unattended. The School Director of Operations controls access to these areas.
• All stored data are protected against destruction or potential damage such as floods, fire, etc. by employing fire-proof cabinets.
• Paper records and electronic customer information are also stored on a secure server whose access is controlled by the Information Security Program Coordinator, Electronic Brain Solutions. Access to this information is password protected and not available to students.
• Staff computers are password protected and students do not have access to them.
• Student and employee PII are not stored on any computer system with a direct internet connection.
• All student information is backed up daily through Electronic Brain Solution. Backup is stored in a
   secure location as determined by the Director of operations. All credit card information is processed through Square.

2.   All electronic transmissions of student and employee PII are secured.
• Social Security information, IRS information, and other sensitive financial data transmitted to SPSC directly from students shall use a secure connection such as a Secure Sockets Layer (SSL) or other currently accepted standard. This is so that the security of such information is protected in transit. Such secure transmissions are automatic. Students are advised against transmitting sensitive data via electronic mail.
• SPSC contractually requires that inbound transmissions of PII, delivered to DDBS via other means, be encrypted or otherwise secured.
• All outbound transmissions of PII are secured in a manner acceptable to the Information Security Program Coordinator. If PII must be transmitted to DDBS by e-mail, such transmissions are password protected or otherwise secured against compromise at the discretion of the Information Security Program Coordinator.

- The Information Security Program Coordinator and third-party services review all student applications to ensure an appropriate level of security both within DDBS and within the third-party server and the IRS.
- Sensitive data must be transmitted to DDBS by electronic mail, such transmissions are password controlled or otherwise protected from theft or unauthorized access at the discretion of the Director of
  Operations.

3.   All paper transmissions of student and employee information by SPSC are secure.
- Any PII delivered by SPSC to third parties are always kept sealed.
- Paper-based student/employee information is never left unattended in an unsecured area.
- All paper transmission of student and employee information is stored in a fireproof locked cabinet
  inside a padlocked records room.

4.   All PII is disposed of in a secure manner.
- The Information Security Program Coordinator (Director of Operations/Business Center Administrator) will supervise the disposal of all records containing PII.
- Paper-based PII is shredded and stored in a secure area until a disposal or recycling service picks it up.
- All hard drives, diskettes, magnetic tapes, or any other electronic media containing PII shall be erased and/or destroyed prior to disposal. All hardware is recycled.
- All PII is disposed in a secure manner after any applicable retention period.

5.   The Information Security Program Coordinator (Director of Operations/Business Center Administrator) maintains an inventory of the school computers and handheld devices on or through which PII may be stored, accessed, or transmitted.

6.   The Information Security Program Coordinator (Director of Operations/Business Center Administrator) develops and maintains appropriate oversight and audit procedures to detect the improper disclosure or theft of student information.

Definitions
- As used in the Gramm-Leach-Bliley Act, "customers" (those to whom SPSC provides services of any kind for).

- For the purposes of this Safeguarding Program, "customer information" is defined as any record containing non-public, personally identifiable financial information regarding any of the school's customers, whether records are maintained on paper, electronically, or by any other means, this security program does not create contractual agreements between the student and any other entity or person.

Applicability
This program applies to all SPSC departments with access to student loan data or other customer information regardless of the purpose or frequency of use and applies to gathering, storing, processing, transmitting, and disposing of customer information. This program also applies to outside service providers, such as loan servicing agents and collection agencies to which student loan data may be transferred or who may gather it on behalf of the school.

Information Security Program Policies and Procedures
By using an updated firewall configuration, protection, and security software (huntress, Webroot, canari, RMM Monitoring, and Pen testing Scanning) SPSC continues to keep the objectives of the Information Security Program. SPSC implements, maintains, and enforces the

following attack and intrusion safeguards to detect, prevent, and respond to attacks, intrusions, or other system failures.

SPSC employs SMART educational management software a fully encrypted school interface. Participating school administrators must be secured with a unique logon ID and password for access.

The Information Security Program Coordinator(s):
SPSC Information Security Program Coordinator is Kanika Free (Director of Operations) is responsible for ensuring SPSC has adequate procedures in place to address any compromise of SPSC's information safeguards. The procedures include appropriate responses to specific types of attacks i.e., hackers, general security failure, denial of access to databases and computer systems, etc.

Based on the information contained in the questions below, there is a mix of hardware and software solutions to help protect and defend SPSC's infrastructure. The coordinators are responsible for the following:

1. Maintaining a working knowledge of appropriate technology for the protection of student PII.
2. EBS trains Spec Ops on a weekly basis along with other training throughout the year.
3. Ensuring that DDBS has installed the most recent updates needed to resolve software vulnerabilities, the Information Security Program Coordinator periodically communicates with SPSC's computer vendor.
4. Making sure updates are installed automatically 4-5 days after they are released. They are monitored for any issues or failures. Third party patching occurs as updates are released.
5. Ensuring SPSC utilization of anti-virus and EDR software that updates automatically.
   Currently using Webroot monitored Anti-virus along with Canauri for ransomware protection and huntress for IDS and EDR.
6. Ensuring that SPSC maintains up-to-date firewalls. Firewall is updated per schedule of releases from the firewall company.
7. Managing SPSC's information security tools for employees and passing along updates about any security risks or breaches. Updates provided related to DDBS's specific infrastructure.
8. In the event of a computer or other technological failure, the Information Security Program Coordinator's will implement previously established procedures to preserve the security, confidentiality, and integrity of student PII. Electronic Brain Solutions will be managing or making repairs so they will know where the data is located and who is accessing it. Once the computer dies, Electronic Brain Solutions will destroy (physically) the hard drive and recycle the computer.
9. Ensures that access to student information is granted only to legitimate and valid users. The student information that resides on the server is access controlled by active directory logins.
10. Notifies students promptly if their PII is compromised.

SPSC has established a way for a person whose "personal identification information" was the subject of a" data breach" in compliance with the mandatory "data breach" notification statutes or regulations to contact students if PII is found to be compromised and a monitoring service that provides "data breach" victims with credit, fraud, public

records or other monitoring alerts through Electronic Brain solutions as well as services that are covered under CNA.

Cyber Incident Response Plan/Policy
In the event of a cyber incident (ransomware, breach, successful phishing attack etc....) the qualified coordinators or IT provider must do the following:

1. Disconnect the computer from the network but keep the system powered on. This may be done with huntress software but if not, it will require someone to physically disconnect the machine.
2. After the qualified individual has been alerted, they will reach out to Electronic Brain Solutions if that has not already been done.
3. The coordinator or Electronic Brain solutions will contact The Hartford which provides the cyber liability policy for instructions on how to proceed.
4. CNA will indicate the next steps and if a 3rd party investigator or response unit will be needed.

Physical Incident Policy
In the event of a physical disaster (fire, flood, etc.) the following must be performed:

1. The coordinator must have access to the school to assess the damage to physical storage as well as technology.
2. After the assessment The Hartford insurance company will be notified.
3. An onsite evaluation of all IT equipment will be performed by the qualified coordinators and Electronic Brain Solutions.
4. After the assessment of any damage by the IT coordinator and Electronic Brain Solutions is performed and if a new server or solution is needed to restore the backup files and get the business applications up and running must be functioning as soon as possible.
5. Physical media will also be evaluated for damage and restoration possibilities.
6. If physical IT equipment is rendered useless, a virtual machine will be created in the cloud and all
   data, and all data and information temporarily migrated to that server.

Incident Management Strategy Policy
A consistent approach to managing information security incidents, consistent with applicable law is in place to handle information security events and weaknesses once they are reported by doing the following:

- reporting any security incidents by documenting the incident completely. Logs and any other evidence of a "security breach" are saved for review.
- Measures to correct any breaches are taken immediately to stop ongoing attacks if found.
- Communicate information security events and vulnerabilities associated with information systems effectively, allowing for appropriate and timely corrective actions.

- **Incident Response:** This formalized plan outlines detailed procedures for incident prevention, detection, assessment, forensics, containment, and recovery activities. This plan aims to mitigate
  computer security risks through comprehensive, structured responses to incidents.
- **Designated Incident Response Personnel:** Designated personnel are responsible for responding to
  incidents. The responsible personnel are responsible for executing the procedures detailed in the Incident Response Plan. These responsibilities include initial response, investigation,

mitigation actions, and coordination with external experts if necessary.

Business Continuity Management Policy/System failure
Backup and recovery plans are documented, distributed, through the organization and easily obtained by office personnel if an event occurs by doing the following:
• Any Backup and recovery options that are presented to SPSC are reviewed and tested regularly to ensure that the best plan is in place per SPSC needs.
• Currently all data is backed up offsite and tested for recoverability in the event of data loss.
• Physical security analysis of both electronic and hardcopy records regularly.

Threat Assessment Policy
This policy is in place to detect and prevent malware, phishing, compromised credentials or passwords along with sabotage and or fire by doing the following:
• The use of the anti-virus with Webroot.
• Constant monitoring with Huntress and anti-ransomware with Canauri.
• Monitoring via RMM.
• Firewall logs and updates.
• Backups both onsite and offsite are performed for disaster recovery.

Records Policy
This policy explains how records are protected including stored information such as: financial records school (restricted), financial records student(private), tax information(restricted), loan applications(restricted),employee HR information(restricted), employee contact information(private), student contact information(private), student account balances(private), website content(public), student personal information(private), parent personal information(private), client personal medical information(private), student financial aid information(private), student grades and attendance(private), emergency contact(private), student paper files(private), student digital files(private). These are the procedures as follows:
• Working with Galactic Scan.
• Penetration testing is done annually.
• All information transferred to SPSC.
• Huntress 24/7
• SOC reviews possible incidents and removes nodes from the network if necessary.
• Traditional anti-virus by Webroot
• Monitoring by RMM.
• Canauri is staffed 24/7 and has alerts for any attempts to remove ransomware.
• Data housed on a specific drive or specific program named SMART which doesn't have encrypted database
  but relies on the security of the server where it resides.

Disposal
SPSC requires the shredding of all paper containing any customer information prior to disposal. In the event of any recycling of personal computers containing customer information, all memory components of such computers will be completely reformatted or otherwise erased for any new use as determined by the department.

Monitoring and detection
All institutional data and computing resources must be continuously monitored to detect any events that may compromise their security. This includes system, security, and operational events. This is to ensure that DDBS identifies potential security incidents promptly and

effectively.

Commitment to Continuous Improvement
SPSC commits to continually improving its response capabilities. This includes regular reviews and updates to the Data Privacy, Cyber Incident & Information Security Response Plan and training programs for the Incident Response Personnel to ensure they are prepared to manage new and evolving threats.

Audits and Monitoring
SPSC reserves the right to perform audits periodic and random checks. This continuous monitoring of its networks and systems will ensure compliance with this cybersecurity policy.

Handling Non-Compliance
Non-compliance with this policy must be reported to the Director of Operations. An assessment of the non- compliance, potential risks involved, and the corrective actions to require preventing future occurrences will be reviewed and if necessary, escalated review and action of the individual (s) involved.

Incident Reporting and Investigation
All breaches of information security, whether actual or suspected, must be immediately reported to the designated personnel. Designated personnel are responsible for initiating an investigation and working with relevant parties to address the breach. A standard procedure for reporting and managing breaches will be outlined in the Incident Response Plan.

Disciplinary Actions
Individuals found in violation of this policy are subject to disciplinary action, which may include, but not limited to, loss of computer and network access and privileges, reprimands, suspension, termination of employment, or legal action, depending on the severity of the breach. Disciplinary measures will be applied consistently and in accordance with DDBS policies.

Compliance Training
To support compliance with this policy, SPSC will provide regular training and awareness programs to all members of the SPSC staff. These programs will cover the importance of information security, the specific requirements of this policy, and the roles and responsibilities of individuals in maintaining security.

Insurance to Cover Data & Information Policy

The CNA Data Breach Response Expense Policy and Procedure
CNA will pay for "data breach expenses" that SPSC incurs because of a "data breach" of personally identifiable information. The following is the procedure in event of a loss you must:
• Report the "data breach" to CNA within 30 days of the discovery of the "data breach."
• Immediately record the specifics of the "data breach' and the date discovered.
• Cooperate with the investigation of the "data breach."
• Assist CNA, upon request in the enforcement of any right against any person or organization which
  may have accessed, stolen or disclosed the information or data giving rise to a "data breach."
• SPSC may not, except at your own cost, voluntarily make a payment, assume any obligation, or incur any
  expense without prior written consent.

- SPSC has 1 year from the date of reporting a "data breach" to initiate services provided to the school.

As soon as possible, CNA should be told the description of how, when and where the "data breach" occurred, including but not limited to all the following, information as it becomes known to you:

1. The method of "data Breach"
2. The approximate date and time of the "data breach"
3. The approximate number of files compromised because of the "data breach."
4. A detailed description of the type and nature of the information that was compromised.
5. Whether or not the information was encrypted, and if so, the level of encryption.
6. Whether or not law enforcement has been notified
7. If available, the place of domicile for all persons whose "personally identifiable information" was the
    subject of a "data breach."
8. If available, who received the information contained in the "data breach."
9. Any other access, information or documentation were reasonably required to investigate or adjust the
    loss.
10. Take all reasonable steps to protect "personally identifiable information" remaining in your care,
    custody, or control.
11. Preserve, and permit us to inspect, all evidence of the "data breach."
12. If requested, permit The Hartford to question SPSC under oath, orally or in writing, at such times as
    may be reasonably required about any matter relating to the insurance or loss, including copies of DDBS books and records. In answering questions in writing SPSC answers must be signed.

The CNA Data Breach Defense Policy and Procedure
CNA will pay for "loss" on behalf of SPSC resulting from a "data breach claim" if the following conditions are met:
- The 'data breach claim" was first made against DDBS during the policy period. A "data breach claim" will be deemed to have been made when notice of such "data breach claim" is received by you or by The Hartford, whichever comes first.
- SPSC had no knowledge of the "data breach" out of which the "data breach" arises.
- The "data breach claim" is reported to The Hartford within 30 days after you receive notice of the claim, but
  in no event later than 30 days after the end of the "policy period."
- The "data breach" must involve "personally identifiable information" that was held by SPSC or on behalf in
  the "coverage territory."
- SPSC must cooperate with The CNA in any investigation, settlement, or defense of the "data breach
  claim", and assist The Hartford, upon their request in the enforcement of any right of recovery regarding any payment of "loss" under SPSC Data Breach Policy. SPSC must execute all papers required and do everything necessary to secure and preserve such rights, including the execution of any documents needed to enable CNA to bring suit in SPSC's name.

  - SPSC may not, except at our own cost, voluntarily make a payment, assume any obligation, or incur any expense without prior written consent.

- SPSC must take all reasonable steps to protect "personally identifiable information" remaining in the care of SPSC.

- SPSC must preserve all evidence of the "data breach".
  SPSC has established crises management services through Electronic Brain Solution that will be able to perform services a way for a person whose "personal identification information" was the subject of a" data breach" in compliance with the mandatory "data breach" notification statutes or regulations to contact students if PII is found to be compromised.

Continuing Evaluation and Adjustment
The Information Security Program will be reviewed annually by the schools' boards, staff, and 3rd party IT company, and will be subject to periodic review and adjustment. Continued administration of the development, implementation and maintenance of the program will be the responsibility of the designated Information Security Program Coordinators, who will assign specific responsibility for technical (IT), logical, physical, and administrative safeguards implementation and administration as appropriate.

Additional Definitions
Covered data and information - for the purpose of this program includes student financial information (defined below) that is protected under the GLBA. In addition to this coverage, which is required under federal law, SPSC chooses as a matter of policy to include in this definition all sensitive data, including credit card information and checking/banking account information received during business hours by the school, whether such information is covered by GLBA. The covered data and information will include both paper and electronic records.

Pretext calling - occurs when an individual attempts to improperly obtain personal information of SPSC customers to be able to commit identity theft. It is accomplished by contacting the school, posing as a customer or someone authorized to have the customer's information, and using trickery and deceit, convincing an employee of the school to release customer-identifying information.

Student financial information - is that information that SPSC has obtained from a student or customer in the process of offering a financial product or service, or such information provided to the school by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student's parent when offering a financial aid package, and other miscellaneous financial services. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format.

Data Breach- means loss, theft, accidental release, or accidental publication of "personally identifiable information", or circumstances objectively giving rise to a substantial risk that such a loss, theft release, or publication has occurred.

Data Breach Expense- Notification expenses to notify a person whose "personally identifiable information" was a subject of a "data breach" notification statutes or regulations.

Loss- meaning civil awards, settlements, and judgments (including any award or prejudgment interest), expenses incurred in the defense of a "regulatory proceeding."

Regulatory Proceeding- meaning an investigation, demand or proceeding, including a request for information, brought by, or on behalf of, the Federal Trade Commission, Federal

Communications Commission or other administrative or regulatory agency, or any federal, state, local or foreign governmental entity in such entity's regulatory or official capacity seeking relief based upon a "data breach.

FTC regulations: 16 CFR 313.3(n) and 16 CFR 314.1–5 Gramm-Leach-Bliley Act: Sections 501 and 505(b)(2) U.S. Code: 15 USC 6801(b), 6805(b)(2)