TONI&GUY HAIRDRESSING ACADEMY'S GLBA INFORMATION SECURITY PROGRAM

Overview: This document summarizes the comprehensive written information security program ("Information Security Program" or the "Program") of TONI&GUY Hairdressing Academy ("TGHA" or "TONI&GUY") mandated by the Federal Trade Commission's Safeguards Rule and the Gramm–Leach–Bliley Act ("GLBA"). The GLBA requires financial institutions to safeguard the nonpublic personal information of their customers. Because TONI&GUY's academies participate in the Department of Education's student financial assistance programs, the Federal Trade Commission considers our academies to be "financial institutions" that are subject to the GLBA. The Program incorporates by reference TGHA's policies and procedures enumerated below and is in addition to any institutional policies and procedures that may be required pursuant to other federal and state laws and regulations, including, but not limited to, the Family Educational Rights and Privacy Act ("FERPA").

Objectives: This Program shall set forth TGHA's efforts to:

1. Identify and assess reasonably foreseeable internal and external risks to nonpublic Customer Information (as defined below);
2. Develop, implement and maintain safeguards in a written Information Security Program to mitigate the risks identified in the risk assessment and ensure the security and confidentiality of Customer Information;
3. Monitor and test the efficacy of the Information Security Program on a regular basis;
4. Protect against any unauthorized use, disclosure, wrongful access of or anticipated threats or hazards to the security or integrity of customer information to prevent substantial harm or inconvenience to any customers;
5. Select and retain third party service providers that can maintain appropriate safeguards under the GLBA;
6. Update the Information Security Program as needed in light of TGHA's testing and monitoring of the Program, any material changes in TGHA's operations or business arrangements or any other circumstances that TGHA knows or has reason to know may have a material impact on our Information Security Program; and
7. Designate an employee or employees who will be responsible for coordinating the Information Security Program.

Definitions:

Consumer – an individual who obtains or has obtained a Financial Product or Service (as defined below) from TGHA for personal, family or household reasons.

Customer – a Consumer who has a continuing relationship with TGHA. Customers may include students, parents, spouses, faculty, staff and third parties.

TGHA'S GLBA Information Security Program

Customer Information – any record having Nonpublic Personal Information (as defined below) about a Customer of TGHA, whether in paper, electronic or other form, which is handled or maintained by or on behalf of our company or our company's affiliates. Examples of handling Customer Information include administering financial aid, processing credit card information and collecting any other form of Customer financial information. Customer Information can include not only a student's financial information, but also parents' annual income or other financial information submitted to our academies.

Financial Institution – a company that offers Consumers Financial Products or Services.

Financial Product or Service – includes student loans, employee loans, activities related to extending credit, financial and investment advisory activities, management consulting and counseling activities, community development activities, and other miscellaneous financial services as defined in 12 CFR § 225.28.

Nonpublic Personal Information – means any personally identifiable financial or other personal information, not otherwise publicly available, that (1) TGHA has obtained from a Customer in the process of offering a Financial Product or Service; (2) has been provided to TGHA by another Financial Institution; (3) TGHA has obtained in connection with providing a Financial Product or Service; or (4) any list, description, or other grouping of Customers (and publicly available information pertaining to them) that is derived using any information listed above that is not publicly available. Examples of personally identifiable financial information include names, addresses, telephone numbers, bank and credit card account numbers, income and credit histories, tax returns, asset statements and social security numbers, both in paper and electronic form.

Service Providers – any person or entity that receives, maintains, processes or otherwise is permitted access to Customer Information by providing services to TGHA. Service Providers may include businesses retained to transport and dispose of Customer Information, collection agencies, and systems support providers, for example.

Designated Customer Information Security Coordinators: The designated Customer Information security coordinators (the "Program Coordinators") are Claire Huntsman, Corporate Counsel and Chief Data Protection Officer, and Will Figuly, Network Administrator. The Program Coordinators shall be responsible for coordinating and overseeing the Program. The Program Coordinators may designate other representatives of TGHA to oversee and coordinate particular elements of the Program as needed. Any questions regarding the implementation of the Program or the interpretation of this document should be directed to the Program Coordinators or their designated representatives.

Scope of Program: The Program applies to any record containing Nonpublic Personal Information about a student or other third party who has a relationship with TGHA, whether in paper, electronic or other form, which is handled or maintained by or on behalf of TGHA or its affiliates.

Elements of the Program:

1. Risk Assessment. TGHA has, as part of the Program, identified and assessed external and internal risks to the security, confidentiality, and integrity of Nonpublic Personal Information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information. The risks TGHA identified are outlined on TGHA's Risk Assessment Worksheet, which is referenced in Section 5 of this Agreement. In implementing the Program, the Program Coordinators will establish procedures for identifying and assessing such risks in each relevant area of TGHA's operations, including:

- **Employee Training and Management**. The Program Coordinators will coordinate with representatives in TGHA's Compliance, Operations, Information Technology, Financial, Human Resources and Financial Aid Departments to evaluate the effectiveness of TGHA's procedures and practices relating to access to and use of student records, including financial aid information. This evaluation will include assessing the effectiveness of TGHA's current policies and procedures in this area. Please refer to the list of all relevant policies and procedures in Section 5 of this Program.

- **Information Systems and Information Processing and Disposal**. The Program Coordinators will coordinate with representatives of TGHA's Information Technology Department to assess the risks to Nonpublic Personal Information associated with TGHA's information systems, including network and software design, information processing, and the storage, transmission and disposal of Nonpublic Personal Information. This evaluation will include assessing TGHA's current policies and procedures relating to network security, acceptable use of TGHA's network, document retention and destruction of data. The Program Coordinators will also coordinate with TGHA's Information Technology Department to assess procedures for monitoring potential information security threats associated with software systems and for updating such systems by, among other things, implementing patches or other software fixes designed to deal with known security flaws.

- **Detecting, Preventing and Responding to Attacks**. The Program Coordinators will coordinate with TGHA's Information Technology Department to evaluate procedures for and methods of detecting, preventing and responding to attacks or other system failures and existing network access and security policies and procedures, as well as procedures for coordinating responses to network attacks and developing incident response teams and policies. In this regard, the Program Coordinators may elect to delegate to a representative of TGHA's Information Technology Department the responsibility for monitoring and participating in the dissemination of information related to the reporting of known security attacks and other threats to the integrity of networks utilized by TGHA.

2. Designing and Implementing Safeguards. The risk assessment and analysis described above shall apply to all methods of handling or disposing of Nonpublic Personal Information, whether in electronic, paper or other form. The Program Coordinators will, on a regular basis, implement safeguards to control the risks identified through such assessments and to regularly test or otherwise monitor the

effectiveness of such safeguards. Such testing and monitoring may be accomplished through existing network monitoring and problem escalation procedures.

TGHA has outlined its risk assessment and analysis, as well as measures in place to reduce said risks on its Risk Assessment Worksheet, which is referenced in Section 5 of this Agreement. TGHA shall further continue the use of or shall implement the following reasonable safeguards as appropriate, as part of our Program:

- Limit information system access to authorized users only;
- Ensure that employees with access to Customer Information are properly trained to maintain the security of the information;
- Train employees to report suspicious activity to supervisors;
- Train employees to maintain the security of their computer systems when they are away from their computers;
- Update system security procedures to include random security testing to ensure authorized employees are maintaining the security of their system;
- Identify and authenticate users appropriately;
- Use passwords to access computer systems that process or contain Customer Information;
- Require password changes to computer systems every ninety (90) days;
- Revoke access to computer systems after a specific number of unsuccessful login attempts;
- Establish incident-handling capability;
- Perform appropriate maintenance on information systems, including installing system updates, implementing patches or performing other fixes designed to deal with known security flaws as needed;
- Protect media, both paper and digital, containing sensitive information;
- Shred and erase Customer Information when no longer needed in accordance with TGHA policy;
- Use firewalls and encrypt information when feasible;
- Use antivirus software to prevent, detect and remove malware on computer systems;
- Maintain physical security by locking rooms and file cabinets where Customer Information is stored;
- Require individuals to sign a confidentiality agreement prior to authorizing access;
- Limit physical access to systems by limiting access to sensitive areas to those individuals with appropriate clearance who require access to those areas in order to perform their job;
- Ensure third party Service Providers are safeguarding Customer Information and monitor to ensure compliance;
- Discourage nonessential use of social security numbers on any forms;
- Conduct periodic risk assessments as required herein;
- Conduct quarterly meetings to review the efficacy of and implement any necessary changes to TGHA's Program;
- Train employees on how to appropriate respond to or report a breach, or potential breach, of Customer Information data;
- Train authorized employees as needed, but, at a minimum, on a quarterly basis to ensure compliance with the Program;
- Assess security controls periodically and implement action plans; and
- Identify, report, and correct information flaws in a timely manner.

3. Overseeing Service Providers. The Program Coordinators shall coordinate with those responsible for the third party service procurement activities among Financial Aid, Information Technology, Accounting and Legal Departments as well as Academy Operations and other affected departments to raise awareness of, and to institute methods for, selecting and retaining only those Service Providers that are capable of maintaining appropriate safeguards for Nonpublic Personal Information of students and other third parties to which they will have access. In addition, the Program Coordinators will work with the Chief Legal Officer to develop and incorporate standard, contractual protections applicable to third party Service Providers, which will require such providers to implement and maintain appropriate safeguards. Any deviation from these standard provisions will require the approval of the Chief Legal Officer. These standards shall apply to all existing and future contracts entered into with such third party Service Providers.

4. Adjustments to the Program. The Program Coordinators are responsible for evaluating and adjusting the Program based on the risk identification and assessment activities undertaken pursuant to the Program, as well as any material changes to TGHA's operations or other circumstances that may have a material impact on the Program.

5. TGHA Policies and Procedures that Protect Customer Information. The following policies and procedures supplement this Program and help to create a comprehensive Information Security Program. The following documents are hereby incorporated by reference into the Program:

- Risk Assessment Worksheet
- Data Classification & Handling Policy & Guide
- Privacy Policy
- Student Records Procedure
- Information Technology Security Policy
- Electronic Data Deletion & Disposal Policy & Procedure
- Payment Card Industry Data Security Policy
- Security Procedure: Risk and Vulnerability Assessments
- Password Policy
- Investigative Contact by Law Enforcement Policy and Procedures
- Electronic Mail Policy
- Wireless Local Area Network (LAN) Systems Policy
- Network Policy
- TONI&GUY Virtual Private Network (VPN) Service on the TONI&GUY Network
- Records Retention Schedule

- *Access to Student Database Acknowledgment*
- Confidential Information & Non-Competition Agreement
- TONI&GUY Hairdressing Academy Right to Privacy
- TONI&GUY Hairdressing Academy Student Catalogue

ACKNOWLEDGEMENT:

I have read and understand the GLBA Information Security Program, as well as the TGHA Policies and Procedures that Protect Customer Information referenced in Section 5 of this document.

Please indicate your acknowledgment with the following by signing below:

_____ _____

Employee Signature Date