

ELITE WELDING ACADEMY INFORMATION SECURITY PLAN

INTRODUCTION

As part of our educational mission, Elite Welding Academy (“EWA”) acquires, develops, and maintains confidential information relating to our students and other customers. The Financial Services Modernization Act of 1999 (also known as the Gramm-Leach-Bliley Act, or “GLBA”), 15 USC § 6801, et seq., “sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity” of such confidential information. 16 CFR 314.1. Toward that end, the GLBA requires financial institutions to:

- Designate an employee or employees to coordinate the information security plan;
- Conduct a risk assessment of likely security and privacy risks;
- Design and implement a security plan to control the risk identified through the risk assessment,
- Oversee service providers and contracts, and
- Evaluate and adjust the security plan

This Information Security Plan (the “Plan”) is intended to comply with these mandates of the GLBA.

OBJECTIVES

The Plan is designed to achieve the following objectives:

- Ensure the security and confidentiality of customer records and information;
- Protect against anticipated threats to the security or integrity of such information; and
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

SCOPE OF THE PLAN

The Plan applies to all nonpublic personal information about a student or other third party who has a customer relationship with EWA, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of EWA. For purposes of the Plan, such nonpublic personal information (“Personal Information”) shall include any of the following:

- Information a student or other third party provides to obtain a financial product or service from EWA;
- Information about a student or other third party resulting from any transaction with EWA involving a financial product or service;
- Information obtained about a student or other third party in connection with providing a financial product or service to that person.

PLAN COORDINATOR

EWA has designated **Bob Reeves** to coordinate the Plan. **Bob Reeves** may designate other EWA representatives to oversee and coordinate particular elements of the Plan. Any correspondence and inquiries relating to the Plan should be directed to **Bob Reeves**.

IDENTIFICATION AND ASSESSMENT OF RISKS

EWA has identified several risks, both internal and external, to the security, confidentiality, and integrity of Personal Information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information. Such risks include:

- Unauthorized use of another user's account and password;
- Unauthorized access to Personal Information through software applications;
- Unauthorized viewing of printed or computer-displayed Personal Information;
- Interception of Personal Information during transmission;
- Physical loss or misplacement of Personal Information;
- Improper destruction of printed material;
- Errors introduced into the system;
- Corruption of information or systems;
- Unauthorized access to Personal Information by employees;
- Unauthorized requests for Personal Information; and
- Unauthorized transfer of Personal Information through third parties.

INFORMATION SAFEGUARDS

Physical Security

EWA limits access to Personal Information to only those employees who have a business reason to know such information. Loan files, account information, and other documents containing Personal Information are kept in file cabinets or rooms that are locked each night. Only authorized employees know combinations and the location of keys. Paper documents that contain Personal Information are shredded at the time of disposal.

Information Systems

Access to Personal Information via EWA's computer information systems is limited to those employees who have a business reason to know such information. Each employee is assigned a user name and password. Databases containing Personal Information, including accounts, balances, and transactional information, are available only to EWA employees in appropriate departments and positions.

Employee Training and Education

To further guard against the risk of unauthorized access to Personal Information, EWA has instituted the following procedures related hiring, training, and managing its employees:

- Checking references or doing background checks before hiring employees who will have access to Personal Information;
- Asking all new employees to sign an agreement to follow the Plan's confidentiality and security standards relating to Personal Information;
- Limiting access to Personal Information to employees who have a business reason to see it;
- Using password-activated screen savers to lock employee computers after a period of inactivity;
- Requiring employees to use "strong" passwords that must be changed on a regular basis;
- Training employees to not share or openly post passwords in work areas;
- Training employees to lock rooms and file cabinets where records are kept;
- Encrypting all sensitive Personal Information when it is transmitted electronically via public networks;
- Referring calls or other requests for Personal Information to designated individuals who have been trained on how your company safeguards personal data;
- Reporting suspicious attempts to obtain Personal Information to designated personnel;
- Regularly reminding employees of the company's policy, and the legal requirement, to keep Personal Information secure and confidential; and
- Imposing disciplinary measures for security policy violations; and
- Preventing terminated employees from accessing Personal Information by immediately deactivating their passwords and user names and taking other appropriate measures.

DETECTING AND MANAGING SYSTEM FAILURES

EWA works to deter, detect, and defend against security breaches. This means taking reasonable steps to prevent attacks, quickly diagnosing a security incident, and having a plan in place for responding effectively.

SERVICE PROVIDERS

“Service provider” refers to any person or entity that receives, maintains, processes, or otherwise is permitted access to Personal Information through its provision of services directly to EWA.

Service providers will be selected based on their ability to maintain appropriate safeguards for Personal Information. To ensure service providers implement and maintain appropriate safeguards, all contracts with service providers shall include the following provisions:

- An explicit acknowledgement that the contract allows the service provider access to Personal Information;
- A specific definition of the Personal Information being provided;
- A stipulation that the Personal Information will be held in strict confidence and accessed only for the explicit business purpose of the contract;
- A guarantee from the contract partner that it will protect the Personal Information it accesses according to commercially acceptable standards and no less rigorously than it protects its own customers’ Personal Information;
- A provision allowing for the return or destruction of all Personal Information received by the contract partner upon completion of the contract;
- A stipulation allowing the entry of injunctive relief without posting bond in order to prevent or remedy breach of the confidentiality obligations of the contract;
- A stipulation that any violation of the contract’s protective conditions amounts to a material breach of contract and entitles EWA to immediately terminate the contract without penalty;
- A provision that requires the service provider to defend, indemnify, and hold EWA harmless for any damages resulting from violation of the contract’s protective conditions;
- A provision allowing auditing of the service provider’s compliance with the contract safeguard requirements; and
- A provision ensuring that the contract’s protective requirements shall survive any termination of the agreement.

CONTINUING EVALUATION AND ADJUSTMENT

The Plan Coordinator shall conduct a periodic internal audit of the Plan in order to evaluate and adjust the Plan in light of relevant circumstances, including changes in EWA's business arrangements or operations, or as a result of testing and monitoring the safeguards.