Program Overview

At Iwaki America Inc., (the "Company"), we are sensitive to the need to protect the security and confidentiality of the Personal Information of our employees contained in our business records. It is our policy that the Personal Information of any of our employees contained in our records is limited to what is reasonably necessary to accomplish legitimate business purposes, and to comply fully with state and federal legal requirements. Our objective in the development and implementation of this comprehensive written Information security program (the "Program") is to create effective administrative, technical and physical safeguards for the protection of Personal Information and to comply with our obligations under 201 CMR 17.00.

For the purposes of this Program, "Personal Information" means a person's first name and last name, or first initial and last name, in combination with any one or more of the following data elements that relate to such resident:

- Social Security number
- Drivers License number or state issued identification card number
- Financial account number, or credit/debit card number with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account

"Personal Information" does NOT include information that is lawfully obtained from publicly available information or from federal, state, or local government records lawfully made available to the general public.

Purpose and Scope

The purpose of this Program is to establish administrative, technical and physical safeguards to protect Personal Information that is owned, licensed, stored, or maintained by the Company, whether such information is contained in paper or electronic records or in any other form. This Program is designed to ensure the security and confidentiality of Personal Information, to protect against anticipated threats or hazards to the security or integrity of Personal Information, and to protect against unauthorized access to or use of Personal Information in a manner that creates a substantial risk of identity theft or fraud.

Administration of Information Security Program

- The Company's Human Resource Director will be the "Information Security Coordinator" (ISC) for this Program

- Responsibilities of ISC:
    - Develop, implement, administer, monitor, review and update this Program from time to time, consistent with the requirements of the Regulation. This includes review of the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing Personal Information.
    - Oversee ongoing employee training and any communications involving this Program
    - Address any information security issues, including employee compliance and access to the Company's Personal Information by former employees, that may arise from time to time, and provide input to the Company regarding the imposition of disciplinary measures for violations of the Program
    - Take all reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such Personal Information consistent with these regulations and any applicable state and federal requirements.
    - Require contractual agreements from third-party service providers that any third-party service provider with access to the Company's Personal Information has the capacity to protect such Personal Information in the manner consistent with this Program and the requirement s of the Regulations and that any such third-party service provider applies protective security measures at least as stringent as those required by the Regulations.
    - The ISC will review incidents of possible or actual breaches and when appropriate will convene a team of employees to form an incident response task force to determine appropriate responses when a breach occurs. The ISC will document all breaches and subsequent responsive actions taken. Records of breaches will be retained in a file in the office of the ISC.

Risk Assessment

The ISC, along with other appropriate employees, has identified and shall continue to identify the reasonably foreseeable internal and external risks to the security, confidentiality and integrity of Personal Information that could result in unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of such information. Among the foreseeable risks are inadvertent destruction, employee misuse of access and external hacks.

Under the direction and supervision of the ISC, the Company shall, on an ongoing basis, review internal and external security risks, and evaluate the effectiveness of and recommend improvements to the Company's Program.

Compliance with the Program
All employees (whether full time, part time, seasonal or temporary) are subject to the applicable requirements set forth in the Program.

Employees *are required* to report any suspicious or unauthorized use of Personal Information to the ISC. Failure to report any such actual or suspected unauthorized access, possession or use of Personal Information when such becomes known to an employee or reasonably should be known, may lead to disciplinary action, up to and including suspension and/or termination.

It is unlawful and against our policy to retaliate against anyone who reports a violation of this Program or who cooperates in an investigation regarding non-compliance with this Program. Any such retaliation will result in disciplinary action by the Company, up to and including termination of employment.

Record Retention
The Company only collects and maintains records and files containing Personal Information of the type, and for the length of time, reasonably necessary to accomplish the Company's legitimate business purpose, or as otherwise necessary for the Company to comply with other local, state or federal requirements. The Company periodically reviews its records, files and form documents to ensure that the Company is not gathering or retaining Personal Information unless there is a compelling reason to do so.

All employees, contractors or consultants are required upon termination or resignation for any reason, or earlier, if upon request of the Company or the ISC, to return or destroy all records and files containing Personal Information of current or former employees or other service providers of the Company, in any form that may at the time of such termination be in their possession or control, including all such information stored on laptops, portable devices (such as thumb drives, zip drives, CDs, DVDs, cell phones or blackberries) or other media, or in files, records, notes or papers.

Handling of Personal Information
Personal Information must be created, stored, disclosed, transmitted and disposed of in the following manner:

- STORAGE: Paper documents containing Personal Information must be stored in a locked or otherwise secured desk, file cabinet, office or controlled area when unattended. All Employees are prohibited from storing Personal Information on Company laptops, portable devices (ie. thumb drives, zip drives, CDs, DVDs, cell phones or blackberries) or other media, or in files, records, notes or papers. If you have a need to store Personal Information via the above-mentioned devices, you must speak to the ISC to determine an alternate method.

- ACCESS: Access to Personal Information in our business records such as names, Social Security numbers, driver's license information and any financial account information is strictly limited to those persons who are required to know such information to perform the functions of their job. Generally, this means the Human Resource Director, Executives, certain IT personnel, and General

Accountant. Certain agents of and service providers to the Company will be given this information but only to the extent necessary for the Company to carry out its responsibilities (e.g. 401(k) provider, health care providers and insurers, our bank for direct deposit transfers, etc).

- TRANSMISSION: All employees are prohibited from transmitting unencrypted Personal Information via email or the internet on Company laptops, portable devices (i.e. thumb drives, zip drives, CD's, DVDs, cell phones or blackberries) or other media. If you need to transmit Personal Information via email or the internet you must consult with the IT Director for alternative methods. Voice communication involving Personal Information must be kept to a minimum and performed in closed or secured locations. Transmission of Personal Information in paper or hard copy from outside the Company, or other removal of Personal Information from the premises, must be done with reasonable precaution to ensure the security of such information and to prevent unauthorized disclosure.

  Employees may not use fax machines for communicating Personal Information unless additional controls are in place to protect the information from unauthorized access or acquisition. For example, ensuring that (i) the recipient's number is correct, and (ii) the recipient is standing by the fax machine waiting to pick up the hard copy.

- DISPOSAL: Personal Information must be disposed of when no longer needed by the Company. Where appropriate, paper documents and other hard copies of records or files containing Personal Information determined by the Company as no longer needed should be disposed of by cross cut shredding so that Personal Information cannot practicably be read or reconstructed. Electronic Personal Information determined by the Company as no longer needed must be destroyed or erased so that Personal Information cannot be read or reconstructed.

Physical and Environmental Controls

- Use and Storage of Files: Employees, contractors or consultants must not keep open documents or files containing Personal Information on their desks when they are not at their desks or in any other unsecured or unattended place. This policy applies to both hard copies and electronic copies of records and files containing Personal Information. A the end of the work day, all filed and other records containing Personal Information must be secured in a manner consistent with this Program and the requirements of the Regulation.
- Blocked Physical Access: The Company prohibits and blocks physical access to records and files containing Personal Information by any individual without authorization to access such records as follows:

  - Only the ISC has physical access to the paper and other hard copies of records containing Personal Information

  - Only the ISC, IT Director and General Accountant have access to the electronic files containing Personal Information

Employees, contractors and consultants are required, upon termination or resignation for any reason, or earlier if upon the request of the Company or the ISC, to surrender all keys, IDs, access codes, badges, business cards and the like that permit access to the Company's premises or to records of the Company containing Personal Information.

- Visitors: Visitors to the Company are prohibited and blocked from accessing any records or files of the Company containing Personal Information.

IT Policies and Procedures

- Electronic Access
    - The Company has in place secure user authentication protocols, including control of User IDs and other identifiers, a reasonably secure method of assigning passwords, and control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect
    - The Company assigns unique identifications plus passwords that are re-designed to maintain the integrity of the security of the access controls, and prohibits the use of vendor supplied default passwords to each authorized active user.
    - The Company will block access to user identification after multiple unsuccessful attempts to gain access.
    - The Company restricts access to authorized users and active user accounts only. Such restrictions allow access to records and files containing Personal Information only to users with a need to access such Personal Information in order to perform their job duties.

IT Security Policies

The Company has reasonably up-to-date firewall protection, operating system security patches, and system security agent software designed to maintain the integrity of the Personal Information. The system security agent software includes malware protection and up-to-date patches and virus definitions installed on all systems processing Personal Information.

Employee's user-IDs and passwords must be changed periodically. Access to electronically stored Personal Information shall be limited at all times to those few employees on a need-to-know basis who shall be assigned a unique log-in ID. Re-log-in is required if you have Personal Information on your computer and the computer is not in use for more than a few minutes. All computer systems and devices used to store or access employee Personal Information are routinely monitored for unauthorized use, possession or access. Violations of this policy may result in disciplinary action up to and including suspension or termination.

Effective Date

This program is effective March 1, 2010.

The Company will review this Program at least annually and reserves the right to change, modify, or otherwise alter this Program at its sole discretion and at any time as it deems circumstances warrant.