**Senior Resources Agency on Aging**

Written Information Security Policy (WISP)

**Statement of Policy**

The objective of Senior Resources Agency on Aging ("The Company") in the development and implementation of this comprehensive written information security policy ("WISP"), is to create effective administrative, technical and physical safeguards for the protection of personally identifiable information (PII) of customers, clients and employees as well as sensitive company information that could harmful if unauthorized access were to occur. The WISP sets forth a procedure for evaluating and addressing electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting PII and sensitive company information.

*The use of the term **employees** will include all of The Company's owners, managers, employees, all independent contractors and temporary employees.*

**Purpose of Policy**

The purpose of the WISP is to better:

1) Ensure the security and confidentiality of **personally identifiable information (PII)** of customers, clients, employees or vendors as well as **sensitive company data** which includes emails, confidential company information (i.e. company expansion plans, manufacturing processes, highly secretive information, etc.), employee information and the like;

2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information; and

3) Protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft, fraud or harm to The Company.

**Scope of Policy**

In formulating and implementing the WISP, The Company has addressed and incorporated the following protocols:

1) Identified reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing PII and sensitive company data.

2) Assessed the likelihood and potential damage of these threats, taking into consideration the sensitivity of the PII and sensitive company data.

3) Evaluated the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risk.

4) Designed and implemented a WISP that puts safeguards in place to minimize identified risks.

5) Implemented regular monitoring of the effectiveness of those safeguards.

**Security Safeguards**

The following safeguards are effective immediately. The goal of implementing these safeguards is to protect against risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing PII or sensitive company data.

**Administrative Safeguards**

1) **Security Officer** - The Company has designated **Executive Director** to implement, supervise and maintain the WISP. This designated employee (the "Security Officer") will be responsible for the following:

    (a) Implementation of the WISP including all provisions outlined in **Security Safeguards.**

    (b) Training of all employees that may have access to PII and sensitive company data. Employees should receive annual training and new employees should be trained as part of the new employee hire process.

    (c) Regular monitoring of the WISP's safeguards and ensuring that employees are complying with the appropriate safeguards.

    (d) Evaluating the ability of any Third Party Service Providers to implement and maintain appropriate security measures for the PII and sensitive company data to which The Company has permitted access, and requiring Third Party Service Providers, by contract, to implement and maintain appropriate security measures.

    (e) Reviewing all security measures at least annually, or whenever there is a material change in The Company's business practices that may put PII and sensitive company data at risk.

    (f) Investigating, reviewing and responding to all security incidents or suspected security incidents.

2) **Security Management** - All security measures will be reviewed at least annually, or whenever there is a material change in The Company's business practices that may put PII or sensitive company data at risk. This should include performing a security risk assessment, documenting the results and implementing the recommendations of the security risk assessment to better protect PII and sensitive company data. The Security Officer will be responsible for this review and will communicate to management the results of that review and any recommendations for improved security arising out of that review.

3) **Minimal Data Collection -** The Company will only collect PII of clients, customers or employees that is necessary to accomplish legitimate business transactions or to comply with any and all federal, state or local regulations.

4) **Information Access** - Access to records containing PII and/or sensitive company data shall be limited to those persons whose job functions requires a legitimate need to access the records. Access to the records will only be for a legitimate job-related purpose. In addition, pre-employment screening should take place to protect PII and sensitive company data.

5) **Employee Termination -** Terminated employees must return all records containing PII and sensitive company data, in any form, that may be in the former employee's possession (including all information stored on laptops or other portable devices or media, and in files, records, work papers, etc.). A terminated employee's physical and electronic access to PII and sensitive company data must be immediately blocked. A terminated employee shall be required to surrender all keys, IDs or access codes or badges, business cards, and the like, that permit access to The Company's premises or information. A terminated employee's remote electronic access to PII and sensitive company data must be disabled; his/her voicemail access, e-mail access, internet access, and passwords must be invalidated.

6) **Security Training** – All employees, which includes all owners, managers, employees, all independent contractors and temporary employees that may have access to PII and sensitive company data, will receive security training. Employees should receive at least annual training, and new employees should be trained as part of the new employee hire process. Employees should be required to show their knowledge of the information and be required to pass an exam that demonstrates their knowledge. Documentation of employee training should be kept and reviewed.

7) **WISP Distribution -** A copy of the WISP is to be distributed to each current employee and to each new employee on the beginning date of their employment. It shall be the employee's responsibility for acknowledging in writing or electronically that he/she has received a copy of the WISP and will abide by its provisions.

8) **Contingency Planning** – All systems that store PII and/or sensitive company data should have the data backed up on, at least, a nightly basis. Data should be encrypted and stored offsite. Disaster Recovery mechanisms and documented procedures should be in place to restore access to PII and sensitive company data as well as any operational systems that The Company relies on. A system criticality assessment should be conducted that defines how critical each of The Company's systems are. Systems that are critical to operations should be restored before non-critical systems. On a periodic basic, data backups, data restoration and Disaster Recovery procedures should be tested and validated.

9) **Security Incident Procedures** - Employees are required to report suspicious or unauthorized use of PII and/or sensitive company data to a supervisor or the Security Officer. Whenever there is an incident that requires notification pursuant to any federal or state regulations, the Security Officer will conduct a mandatory post-incident review of the events and actions taken in order to determine how to alter security practices to better safeguard PII and sensitive data.

10) **Emergency Operations** – Procedures should be in place to define how The Company will respond to emergencies. Procedures should include employee contact information, critical vendor contact information, important vendor account information as well as any emergency operating procedures.

11) **Data Sensitivity Classification** – All data that The Company stores or accesses should be categorized in terms of the sensitive nature of the information. For example, PII and sensitive company data might have a very high sensitivity and should be highly protected. Whereas publicly accessible information might have a low sensitivity and requires minimal protection.

12) **Third Party Service Providers** - Any service provider or individual ("Third Party Service Provider") that receives, stores, maintains, processes, or otherwise is permitted access to any file containing PII and/or sensitive company data shall be required to protect PII and sensitive company data. The Third Party Service Providers must sign service agreements that contractually hold them responsible for protecting The Company's data. Examples include third parties who provide off-site backup of electronic data; website hosting companies; credit card processing companies; paper record copying or storage providers; IT / Technology Support vendors; contractors or vendors working with customers and having authorized access to PII and/or sensitive company data.

13) **Sanctions** - All employment contracts, where applicable, should be amended to require all employees to comply with the provisions of the WISP and to prohibit any nonconforming use of PII and/or sensitive company data as defined by the WISP. Disciplinary actions will be taken for violations of security provisions of the WISP (The nature of the disciplinary measures may depend on a number of factors including the nature of the violation and the nature of the PII and/or sensitive company data affected by the violation).

14) **Bring Your Own Device (BYOD) Policy** – The Company may allow employees to utilize personally owned devices such as laptops, smartphones and tablets. If allowed, proper safeguards must be implemented to protect PII and sensitive company data that may be accessed or stored on these devices. Employees must understand what are the requirements for using personally owned devices and what safeguards are required.

**Physical Safeguards**

15) **Facility Access Controls** – The Company will implement physical safeguards to protect PII and sensitive company data. There will be physical security on facilities / office buildings to prevent unauthorized access. All systems that access or store PII and/or sensitive company data will be physically locked. Employees will be required to maintain a "clean desk" and ensure that PII and/or sensitive company data is properly secured when they are not at their desk. The Security Officer will maintain a list of lock combinations, passcodes, keys, etc. and which employees that have access to the facilities and PII and/or sensitive data. Visitors will be restricted from areas that contain PII and/or sensitive company data.

16) **Network Security** – The Company will implement security safeguards to protect PII and sensitive company data. Safeguards include; isolating systems that access or store PII and/or sensitive company data, the use of encryption on all portable devices, physical protection on portable devices, ensuring that all systems run up-to-date anti-malware, implementing network firewalls, performing periodic vulnerability scans, capturing and retaining network log files as well as ensuring that servers and critical network equipment are stored in an environmentally safe location.

**Technical Safeguards**

17) **Access Control** - Access to PII and sensitive company data shall be restricted to approved active users and active user accounts only. Employees will be assigned unique user accounts and passwords. Systems containing PII and sensitive company data should have automatic logoff procedures to prevent unauthorized access.

18) **Computer Use** – All employees will be given a Computer Use Policy that defines acceptable and unacceptable use of The Company's computing resources. Employees should be required to sign the Computer Use Policy to acknowledge acceptance of the policy.

19) **Data Disposal** - Written and electronic records containing PII and sensitive company data shall be securely destroyed or deleted at the earliest opportunity consistent with business needs or legal retention requirements.

20) **System Activity Review** - All systems that store or access PII and sensitive company data should utilize a mechanism to log and store system activity. Periodic system activity reviews should occur and identify unauthorized access to PII and sensitive company data. Any unauthorized access should be reported to the Data Security Coordinator.

21) **Encryption** - To the extent technically feasible all portable devices that contain PII and sensitive company data should be encrypted to protect the contents. In addition, encryption should be used when sending any PII and sensitive company data across public networks and wireless networks. Public networks include email and Internet access.

## Appendix A – WISP Employee Acknowledgement Form

I have read, understand, and agree to comply with the Written Information Security Policy (WISP), rules, and conditions governing the security of PII and sensitive company data. I am aware that violations of the WISP may subject me to disciplinary action and may include termination of my employment.

By signing this Agreement, I agree to comply with its terms and conditions. Failure to read this Agreement is not an excuse for violating it.

| | |
|---|---|
| _____ | _____ |
| Signature | Date |
| _____ | _____ |
| Employee's Supervisor Signature | Date |