Written Information Security Plan (WISP)

for

HR Knowledge, Inc.

This document has been approved for general distribution.

Last modified January 01, 2014

I. PLAN OBJECTIVE

The objective of this comprehensive written information security plan ("Plan"), is to create effective administrative, technical and physical safeguards by HR Knowledge, Inc. ("Company"), located in Mansfield, MA for the protection of personally identifiable information ("PII") of residents of the Commonwealth of Massachusetts, and to comply with obligations under 201 CMR 17.00 "Standards for The Protection of Personal Information of Residents of the Commonwealth", as well as any other federal, state and international regulations and standards. This plan is reviewed periodically and amended as necessary to protect personal information.

This Plan sets forth Company procedure for evaluating electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting personal information of residents of the Commonwealth of Massachusetts. For purposes of this Plan, "personal information" means a Massachusetts resident'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: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or 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; provided, however, that "personal information" shall 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.

II. PURPOSE

The purpose of this Plan is, to the extent possible, to:

A. Ensure the security and confidentiality of personal information collected by and in the possession of the Company.

B. Protect against potential threats or hazards to the security or integrity of such information.

C. Protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud.

III. SCOPE OF PLAN

In formulating and implementing the Plan, the Company will take reasonable steps to:

A. Identify reasonably foreseeable internal and external threats to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information.

B. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information. C. Evaluate the sufficiency of existing policies, procedures,

customer information systems, and other safeguards in place to control risks.

D. Consider and implement measures to minimize those risks, consistent with the requirements of 201 CMR 17.

E. Regularly monitor the effectiveness of those safeguards.

IV. DATA SECURITY COORDINATOR

In compliance with 201 CMR 17, the Company has designated Gary Cowan as the Data Security Coordinator to implement, supervise and maintain the Plan. The Data Security Coordinator will be responsible for the following:

a. Implementation of the Plan.

b. Verifying training of employees.

c. Monitoring and testing of employee compliance with the Plan's policies and procedures.

d. Evaluating the ability of any third-party service provider to protect the personal information to which the Company has permitted it access; and taking necessary and reasonable steps to ensure that such third party service provider applies protective security measures at least as stringent as those required to be applied to such information under 201 CMR 17.00.

e. Reviewing the scope of the security measures in the Plan at least annually, or whenever there is a material change in the Company's business practices that may implicate the security or integrity of records containing personal information.

f. Conducting an annual training session for all owners, managers and employees, including temporary and contract employees who have access to personal information on the elements of the Plan. All attendees at such training sessions are required to certify their attendance at the training, and their familiarity with the firm's requirements for ensuring the protection of personal information.

V. INTERNAL RISKS

To combat internal risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks the Company has implemented the following mandatory policies and procedures:

A. The Company maintains that personal information or other sensitive information will be kept in filing

cabinets, servers, desktop PCs and specific laptop computers to be identified by the Company. Physical safeguards will include lock and key; logical safeguards will include perimeter firewalls and data encryption.

B. The Company will provide regular network security reviews in which all server and computer system logs are evaluated for any possible electronic security breach. These reviews will be performed at least every thirty (30) days. Additionally, all employees will be trained to watch for any possible physical security breach, such as unauthorized personnel accessing file cabinets or computer systems.

C. A copy of this Plan will be distributed to each employee who shall, upon its receipt, acknowledge in writing that he/she has received the copy.

D. A version of this plan will be made available on the company Web site or upon request to those who have a legitimate need to verify the Company's legal compliance.

E. The Data Security Coordinator or his authorized representative will immediately train all existing employees on the detailed provisions of the Plan. All employees will be subject to periodic reviews by the Data Security Coordinator to ensure compliance.

F. All employees are responsible for maintaining the privacy and integrity of the Company's PII. Any paper record containing PII must be kept behind lock and key when not in use. Any computer file stored on the company network which contains personal information will be kept password-protected and/or encrypted.

G. No personal information will be disclosed without authenticating the receiving party or without securing written authorization from the individual whose personal information is contained in such disclosure.

H. Employees are prohibited from keeping open files containing personal information on their desks when they are not at their desks.

I. At the end of the work day, all files and other records containing personal information must be secured by employees in a manner that is consistent with the Plan's rules for protecting the security of personal information.

J. Visitors' access is restricted to a single entry point for each building in which personal information is stored, and visitors shall be required to present a photo ID, sign-in and/or wear a plainly visible "GUEST" badge or tag. Alternatively, visitors must be accompanied by an escort within any area of the company.

K. When disposing of paper records containing personal information, a cross-cut shredder or outside shredding service will be used. Similar appropriate electronic methods will be used for disposing of electronic media.

L. The amount of personal information collected as well as access to records containing personal information shall be limited to those persons who are reasonably required to know such information in order to accomplish a legitimate business purpose or to enable us to comply with other state or federal regulations.

M. The Company will take all possible measures to ensure that employees are trained to keep all paper and electronic records containing personal information securely on- premises at all times. When there is a need to bring records containing personal information off-site, only the minimum information necessary will be brought. Electronic records will be encrypted; paper records will be kept behind lock and key. Records brought off-site should be returned to the Company office as soon as possible.

N. Under no circumstances are documents, electronic devices, or digital media containing any personal information to be left unattended in an employee's car, home, or in any other potentially insecure location.

O. Any employee who willfully discloses personal information or fails to comply with these policies will face immediate disciplinary action that includes a written warning plus other actions up to and including termination of employment.

P. Any terminated employees' computer access passwords will be disabled before or at the time of the termination process. Physical access to any documents or resources containing personal information will also be immediately discontinued. Such 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 firm's premises or information. Moreover, such terminated employee's remote electronic access to personal information will be disabled; his/her voicemail access, e-mail access, Internet access, and passwords will be invalidated. The Data Security Coordinator and/or his designee shall maintain a highly secured master list of all lock combinations, passwords and keys.

Q. The Company periodically shares personal information in the form of employment records, pension and insurance information, and other information required to be a responsible employer. The Company may share this personal information with the state and federal tax authorities, a bookkeeping service, a payroll service, a CPA firm, legal counsel, and/or business advisors. An IT support company may occasionally see personal information in the course of service. Access to personal information by these third-party organizations will be kept to the minimum required to conduct business.

Any third party service provider that does require access to information must be compliant with 201 CMR 17. The Company requires each of these organizations to provide a letter annually, signed by their CEO or other authorized individual, stating that they follow a written information security plan (WISP) that fully complies with 201 CMR 17. The only exception is the state and federal tax authorities, which we assume are compliant, since they must comply with laws that are stricter than 201 CMR 17.

R. The Company is committed to collecting only the minimum amount of personal information

necessary for its business operations; old information is also disposed of securely after no more than seven years or after whatever period is required by federal and state data retention requirements.

S. The Data Security Coordinator has identified and documented the locations where personal information is stored on the Company network.
   i. Servers
   ii. Filing Cabinets
   iii. Desktop PC Workstations
   iv. Laptop Computers
   v. Online (Web-based) applications
   vi. Database Applications, such as Intuit QuickBooks

T. Laptop hard disks and USB-based storage media are encrypted using software such as Microsoft BitLocker.

U. The Company stores backups on hard disks and at an offsite data center using strong encryption techniques provided by the manufacturer of the backup software.

V. The Data Security Coordinator or his designee will monitor and review access, security and handling of personal information by employees. Company offices and filing cabinets containing PII are kept locked third-parties are not allowed physical access to data or records. Paper files that are not currently in use are kept in locked filing cabinets. In addition, electronic records are kept in databases and on servers which are behind multiple layers of electronic security.

W. The Data Security Coordinator or his approved representative will regularly monitor and assess all of the Company's information safeguards to determine when upgrades may be necessary.

X. If there is an incident that requires notification under the provisions of 201 CMR 17, there shall be a mandatory post-incident review by the Data Security Coordinator of events and actions taken, if any, with a view to determining whether any changes in operations are required to improve the security of personal information for which Company is responsible. Records of this will be kept on file with our Written Information Security Plan.

VI. EXTERNAL RISKS

To combat external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the Company has implemented the following mandatory policies and procedures.

A. The Company shall implement and maintain secure authentication protocols to gain access to network that include:

a. Protocols for control of user IDs and other identifiers.

b. A secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices.

c. Unique strong passwords are required for all user accounts.

d. Control of 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.

e. Restriction of access to active users only.

f. Blocking of logon access after multiple, unsuccessful attempts to gain access to a resource.

B. The Company shall implement and maintain secure access control measures that include:

a. Only employees that need access to the personal information are given access to the storage locations containing such information.

b. Each person shall have a unique password to the computer network, which may be changed at will by the individual without disclosure of such password to any other individual.

c. User passwords will be subject to an enforced password policy.

C. Company policy is that PII will not be emailed in plain-text over an unsecured medium such as the Internet unless the message is sent using an encryption method such as TLS or if the specific PII is encrypted using an alternative method.

D. The Company makes wireless access available to its users. All wireless access points are configured to use strong encryption. The company does not provide open (guest) access on its corporate network and will not support WEP.

E. The Data Security Coordinator or his representative performs a network security review at least every thirty (30) days in order to detect possible threats or breaches in network security.

F. Information regarding audits, audit trails and other secure information will be restricted to the Data Security Coordinator and other authorized personnel as designated by the President or owner of the Company.

G. The Company uses at least a third-generation, business-class firewall between the Internet and the private network. This firewall is secured and maintained by the Company's IT provider.

H. Operating system patches and security updates are installed at least every thirty (30) days to all Company servers.

I. The Company enforces the use of a software-based firewall on all workstations. The Company will configure firewall "exceptions" if/when needed based on the business requirements.

J. The company supports only Web browsers that have built-in antiphishing techniques.

K. The Company provides remote access using mechanisms that encrypt not only the traffic between the client and server, but also the authentication requests (ID and password).

L. The Company conducts a thorough security review of any computer that it adds to the network, patching it with the latest updates and then providing the user with his/her logon ID and password.

M. The Company or a certified, third-party organization erases the hard disk of any computer that the Company intends to permanently remove from the network. If a hard drive is unable to be erased because it is broken, the Company or third-party will destroy its electrical leads and dispose of it in the trash, or send it to a disk destruction facility.

N. The Company runs licensed antivirus software which is kept updated on all servers and workstations. Virus definition updates are installed on a regular basis, and the entire system is tested at least once per month.

O. All employees are responsible for maintaining the privacy and integrity of the Company's PII. All employees have been trained that any paper record containing personal information must be kept behind lock and key when not in use. Any computer file containing personal information will be encrypted if it needs to be transmitted or moved off the corporate network. The Data Security Coordinator trains all new employees on this policy, and there are also periodic reviews for existing employees.

VII. NOTIFICATION OF SECURITY BREACH

If the Company's Data Security Coordinator determines that personal information has been stolen or lost, s/he will notify the Office of Consumer Affairs & Business Regulation (OCABR) and the Attorney General's office, describing the theft or loss in detail, and work with authorities to investigate the issue and to protect the victims' identity and credit. To the extent possible, the Data Security Coordinator will also notify the victims of the theft so that they can protect their credit and identity.

VIII. IMPLEMENTATION

Effective this date January 1, 2014, HR Knowledge Inc. has developed and implemented this written information security plan (WISP) in compliance with Massachusetts Regulation 201 CMR 17.

Jeffrey Garr

January 1, 2014
Date

CEO
Title