Written Information Security Plan

V.1.0 DATED: AUGUST 27, 2012

I. Objective

Russell Reynolds Associates' ("RRA" or the "Company") has legitimate business reasons for handling personal information relating to our employees for employment purposes, candidates and individual contacts of our corporate clients. We collect and process resumes and related information on candidates and information on job openings, recruiting requirements and contact information from our clients who are looking for candidates. Except with respect to information about our employees maintained for payroll purposes, the Company does not ordinarily collect Personal Information (as defined below) in the regular course of our business.

Our objective, in the development and implementation of this comprehensive Written Information Security Plan ("WISP" or "Plan"), is to create effective administrative, technical and physical safeguards for the protection of personal information of employees, clients and candidates, and to comply with the Company's obligations under the Massachusetts regulations found at 201 CMR 17.00 et seq. and any other similar regulations applicable to our business (the "Regulations"). The Plan sets forth our policies for evaluating our electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting Personal Information. This Plan is subject to change at the discretion of RRA.

For purposes of this Plan, "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 individual: (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 person'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 the plan is to:

- Ensure the security and confidentiality of Personal Information;
- Protect against any anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of such information in a manner that could result in substantial harm or inconvenience to our employees, clients or candidates.

III. Plan

In formulating and implementing the Plan, we will:

- Identify reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing Personal Information;
- Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Personal Information;
- Evaluate the sufficiency of existing policies, procedures, information systems, and other safeguards in place to control risks; and
- Design and implement a plan that puts safeguards in place to minimize those risks, consistent with the Regulations.

IV. Administration

RRA has identified the combined efforts of the Chief Information Officer, along with the General Counsel, as the Data Security Managers with the following responsibilities:

- Initial implementation of the Plan;
- Oversee ongoing employee training and any communications involving this Plan;
- Regular testing of the Plan's safeguards;
- Take all reasonable steps to verify 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 Plan and the Regulations and that any such third party service provider applies protective security measures at least as stringent as those required by the Regulations.
- Review the scope of the security measures in the Plan at least annually, or whenever there is a material change in our business practices that may implicate the security or integrity of records containing Personal Information.
- Protect Personal Information collected as written or digital data by ensuring all employees handling Personal Information data are properly trained.
- Ensure company-wide compliance with this policy.

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 following measures are mandatory and are effective immediately.

- The amount of Personal Information collected must be limited to that amount reasonably necessary to accomplish our legitimate business purposes, or necessary to us to comply with other state or federal regulations.
- Access to records containing Personal Information shall be limited to those persons who are reasonably required to know such information in order to accomplish legitimate business purpose or to enable the Company to comply with other state or federal regulations.
- Electronic access to user identification after multiple unsuccessful attempts to gain access must be blocked.
- All security measures shall be reviewed at least annually, or whenever there is a material change in our business practices that may reasonably implicate the security or integrity of records containing Personal Information. The Data Security Managers shall be responsible for this review and shall fully apprise management of the results of that review and any recommendations for improved security arising out of that review.
- Terminated employees must return all records containing Personal Information, in any form, which may at the time of such termination be in the former employee's possession (including all such 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 Personal Information must be immediately blocked. 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 Company's premises or information. Moreover, such terminated employee's remote electronic access to Personal Information must be disabled; his/her voicemail access, e-mail access, internet access, and passwords must be invalidated.

- Current employees' passwords must be changed periodically. Currently, our employees are required to change their passwords every 45 days.
- Access to Personal Information shall be restricted to active employees and active user accounts only.
- Employees are prohibited from keeping open files containing Personal Information on their desks when they are not at their desks.
- When unattended, all files and other records containing Personal Information must be secured in a manner that is consistent with the Plan's rules for protecting the security of Personal Information.
- Each department shall develop rules (bearing in mind the business needs of that department) that ensure that reasonable restrictions upon physical access to records containing Personal Information are in place, including a procedure that sets forth the manner in which physical access to such records in that department is to be restricted; and each department must store such records and data in locked facilities, secure storage areas or locked containers.
- Access to electronically stored Personal Information shall be electronically limited to those employees having a unique log-in ID; and re-log-in shall be required when a computer has been inactive for more than 35 minutes.
- Visitors' access must be restricted. All visitors to the Company must be registered at reception and must be accompanied by an employee or other service provider of the Company. Visitors of the Company are prohibited and blocked from accessing any records or files of the Company containing Personal Information.

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 following measures are mandatory and are effective immediately.

- There must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the Personal Information, installed on all systems processing Personal Information.
- There must be reasonably up-to-date versions of system security agent software; which must include malware protection and reasonably up-to-date patches and virus definitions, installed on all systems processing Personal Information.
- Any email containing Personal Information should be encrypted. Additionally, with respect to the Personal Information of Massachusetts's residents (or residents or citizens of any other jurisdictions with similar regulations) stored on laptops or other portable devices, to the extent technically feasible, all such Personal Information will be encrypted, as must all records and files containing such Personal Information transmitted across public networks or wirelessly, to the extent technically feasible.
- All computer systems must be monitored for unauthorized use of or access to Personal Information.
- There must be secure user authentication protocols in place, including: a) protocols for control of user IDs and other identifiers; b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices; c) 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; d) restriction of access to active users and active user accounts only; e) blocking of access to user identification after multiple unsuccessful attempts to gain access; and f) the secure access control

measures in place must include assigning unique identifications plus passwords, which are not vendor-supplied default passwords, to each person with computer access to Personal Information.

VII. Compliance With Plan

A. Compliance. All employees (whether full-time, part-time, substitute, seasonal, or temporary) and independent contractors, consultants, volunteers and other representatives of the company (the "consultants and other representatives") are subject to the applicable requirements set forth in this Plan.

B. Non-Compliance. Instances of non-compliance with this Plan must be reported immediately to the Data Security Managers. Violations may result in disciplinary action by the Company, up to and including termination of employment.

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

VIII. Record Retention

A. 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 purposes, or as otherwise necessary for the Company to comply with other local, state, or federal regulations or requirements. The Company periodically reviews its records, files, and form documents to ensure that the Company is not gathering and retaining Personal Information unless there is a compelling need to do so.

IX. Handling of Personal Information

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

A. Creation. Upon creation of paper and electronic documents and files that contain Personal Information, such documents and files must be marked as "Confidential."

B. Storage. Paper documents containing Personal Information must be stored in a locked or otherwise secured desk, file cabinet, office, or controlled area when unattended. Storage of electronic Personal Information should be kept to a minimum. Any questions regarding the Company's encryption technology should be directed to the Data Security Managers.

C. Access, Sharing, and Disclosure. Access to, sharing, and disclosure of records or files containing Personal Information is limited to those persons who are reasonably required to know such information in order to accomplish the Company's legitimate business purposes or to enable the Company to comply with other local, state, or federal regulations or requirements.

E. Transmission. Voice communications 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 form outside of the Company, or other removal of Personal Information from the Company's premises, must be done with reasonable precaution and in accordance with any applicable Company procedures and/or rules to ensure the security of such information and to prevent unauthorized disclosure.

F. 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 to be no longer needed should be disposed of by cross-cut shredding, incineration, pulping, redaction, or burning, so that Personal Information cannot practicably be read or reconstructed. Electronic Personal Information determined by the Company to be no longer needed must be destroyed or erased so that Personal Information cannot practicably be read or reconstructed.

X. Physical and Environmental Controls

A. Use and Storage of Files. Employees, consultants, and other representatives of the Company 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, unattended place. This policy applies to both hard-copies and electronic copies of records and files containing Personal Information. At the end of the work day, all files and other records containing Personal Information must be secured in a manner that is consistent with this Plan and the requirements of the Regulations.

XI. Security Awareness

A. Training. The Company provides education and training regarding this Plan to all employees who will have access to Personal Information through their employment to the Company.

B. Consultants. Volunteers. Third-Party Service Providers. The Company communicates its relevant policies and procedures under this Plan to its third-party providers, consultants and other representatives who will have access to Personal Information through their services to the Company.

XII. Third-Party Service Providers

A. Vetting Process. Before engaging a third-party service provider who will have access to Personal Information, the Company conducts reasonable due diligence to assess whether a prospective third-party service provider is capable of safeguarding Personal Information in the manner required by this Plan. Due diligence efforts may include, but are not necessarily limited to, discussions with the prospective third-party service provider's personnel, reviewing the prospective third-party service provider's privacy and/or information security policies, and/or requesting the prospective third-party service provider to complete a security questionnaire or otherwise answer security-related questions. The Company may also enter into a contractual agreement with its third-party service providers to protect Personal Information disclosed to such service providers by the Company.

B. Monitoring. The Company periodically reviews and monitors the performance of its third-party service providers who have access to the Company's systems and/or Personal Information in order to ensure that each such third-party service provider is applying protective security measures at least as stringent as those required by this Plan to be applied to such information.

XIII. Risk Assessment and Incident Management

A. Identifying Records and Files Containing Personal Information. The Company will regularly evaluate its paper, electronic, and other records, electronic systems, and storage media (including laptops and portable devices used to store Personal Information) to determine which records, files, and systems contain Personal Information.

B. Ongoing Risk Assessment. The Company will, on a periodic basis, (i) conduct a review to identify reasonably foreseeable internal and external risks to the security, confidentiality, or integrity of any electronic, paper, or other records containing Personal Information; (ii) assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Personal Information; (iii) evaluate the sufficiency of this Plan to control those risks; and (iv) revise this Plan to minimize those risks, consistent with the requirements of the Regulations. This risk assessment will include, but may not be limited to, an assessment of internal and external risks associated with ongoing employee training, employee compliance with this Plan, and means for detecting and preventing security system failures.

C. Review of Plan. The Company conducts a formal review of this Plan at least annually, and whenever there is a material change in the Company's business practices that may reasonably implicate the security or integrity of records or files containing Personal Information.

D. Reporting Obligation. Employees, consultants, and volunteers are required to report any security violations, breaches of security, or suspicious or unauthorized use of Personal Information contained in records or files of the Company to the Data Security Managers.

E. Incident Review. The Company documents any responsive actions taken in connection with each security incident. The Company conducts a prompt review of any security incident, including incidents that require notification under the Regulations, and determines whether any changes in this Plan are required to improve the security of records and files containing Personal Information. If the Company determines that particularly sensitive personal data has been accessed without authorization, we will work with legal counsel to determine what our contractual and statutory incident response and notifications obligations are, and cooperate with law enforcement and our clients to ensure that data is protected as much as reasonably possible. Also, we will work with authorities to investigate any crime and to protect the victim's identity and credit. To the extent possible, we will also warn – or work with our clients and vendors to warn – any victims of data theft so that they can protect their credit and identity.