WORLDWIDE INFORMATION, LLC.
PRIVACY AND SECURITY POLICY

We at WORLDWIDE INFORMATION, LLC recognize the importance of privacy and the sensitivity of personal information. We are committed to protecting personal information we hold in accordance with law. Our Privacy and Security Policy outlines how we manage personal information and safeguard privacy. By accessing our services or by accessing our website, or both, you acknowledge and fully understand this Privacy and Security Policy and freely consent to the information collection and use practices described in this Privacy and Security Policy.

Personal Information

We define "Personal information" as information about an identifiable individual, employee or subject. It also includes but is not limited to "Account" and or Credit Card/Payment information. It does not include the name, title or business address or telephone number of an employee of an organization.

Personal Information - Collection

WORLDWIDE INFORMATION provides services to a wide range of clients. In doing so, often collect and use personal information. In addition, WORLDWIDE INFORMATION at times may send to individuals' information and marketing materials concerning relevant developments in our various areas of service.

We collect personal information fairly and in accordance with the law. Generally, we collect personal information directly from individuals to which it relates. Such collection may be done at the start of our relationship with a client as well as during our relationship.

Occasionally we may obtain information about individuals from other sources including, for example:

- from a government agency or registry;
- other service providers who serve our clients
- The "Internet"

Consent

In most cases, if we collect, use, or disclose personal information, we will obtain consent from the individual to whom it relates. Sometimes we will ask for consent in writing, but in some cases, we may accept oral consent. Sometimes consent may be implied through conduct with us or the nature of our services. Should consent be withdrawn, it may impact on our ability to provide our services. Withdrawal of consent should always be done in writing.

Use of Personal Information

We use personal information to provide services, to administer our client databases, and occasionally to include individuals in our information distribution and marketing activities. The preceding includes the following uses: 1) we may share certain aggregated demographic information with our business partners regarding the users of our websites; 2) we may share certain personally identifiable consumer information with our business partners regarding applicants and other consumers; and 3) we may from time to time communicate service offerings to applicants and other consumers via our co-marketing partners.

At no time shall any personal/private and or PII information be left on an internal company answering device and or service, nor shall any employee/agent of company be allowed to leave like information on any other internal and or external recording device, unless approved in advance, in writing, by management.

Disclosure of Personal Information

Subject to the above provision titled "Use of Personal Information", we will not disclose personal information we collect from you to third parties without your permission except to the extent necessary including:

- to fulfill your requests for services;
- when the relevant individual has consented to the disclosure;
- when we are required by law to do so, or required by a warrant, a subpoena, or rules of court to do so;
- when the services we are providing requires us to give a client's personal information to third parties, his or her consent will be implied, unless he or she tells us otherwise;
- where it is necessary to protect our firm from liability or to collect fees or disbursements;
- where the disclosure is in connection with a merger, acquisition, or liquidation of our company; or
- if we engage a third party to provide administrative services to us (like computer back-up services, archival file storage, or insurance) and the third party is bound by obligations regarding privacy which are consistent with this Policy.

Breach Notification

In the event of a potential breach of protected information or "PII", Worldwide Information will investigate the incident consistent with its Security Rule, security incident procedures (if applicable). Steven R. Russo, the firms' Executive Vice President, will lead the team utilizing one or more team members of the that will participate in such investigation and report relevant facts to the Steven for purposes of determining whether notification will be required.

In determining whether notification is required, the Steven may consult with any additional employees, agents, contractors, consultants, or other individuals reasonably necessary to determine whether Worldwide Information has a duty to notify individuals and or clients about a breach. Legal counsel may be utilized for advice as deemed necessary.

Investigation

In the event there is suspicion, and or detection, or someone otherwise learns of a security violation of electronic or paper files, this information will be forwarded immediately to Steven Russo, and he will investigate the security incident consistent with Worldwide Information's Policies and Procedures. If the incident involves records containing PII, other workforce members who learn of an incident involving unauthorized access to PII (whether in electronic or paper form) will also notify the Steven of the component where the violation may have occurred.

Updating Information

Since we use personal information to provide our services, it is important that the information be accurate and up-to-date. If during a service relationship, any personal information changes, we ask that clients please inform us so that we can make any necessary changes. We may also periodically inquire of clients whether their personal information is accurate and up-to-date.

Securing Personal and Other Information

WORLDWIDE INFORMATION, LLC takes precautions to ensure that personal information is kept safe from loss, unauthorized access, modification or disclosure. Among the steps taken to protect personal information are:

- premises security;
- deploying technological safeguards including security software and a variety of firewalls to prevent unauthorized computer access or "hacking" both internally and externally;
- internal password and security policies;
- No sensitive information shall be transferred other than by Facsimile, manual entry into client/vendor systems, or CertainSafe to ensure the highest levels of protection and encryption.
- we limit the storage of information we maintain regarding subjects to the most minimal time frame necessary to complete a "Batch process" or as otherwise directed by law;
- Data shall never be stored on removable media devices at any time

In the unlikely event of a security and or data breach of any kind or should there be any question as to whether a security breach has occurred, you are to report the incident to your immediate supervisor, who intern will immediately write up the incident and communicate directly to a member of the executive team. That member will engage legal counsel for guidance as necessary or deemed necessary.

WORLDWIDE INFORMATION implements and maintains a comprehensive information security program designed to ensure the security and confidentiality of sensitive data, including but not limited to subscriber codes, security digits, passwords and other PII information, and to protect against anticipated threats and unauthorized access to such information. At any time "Information" or Data" is not being utilized and or processed in the presence of an authorized member of our team, it is stored behind locked access areas to limit and minimize potential risk exposure**.**

Passwords – Use and Storage

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in a compromise of our entire network. As such, all employees (including contractors and vendors with access to our systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their password. (See Physical Protection Policy for additional information). The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any company facility, has access to the company network and/or network, or stores any non-public and or PII personal Information.

General

• All systems-level passwords (e.g., root, enable, network administrator, application administration accounts, etc.) must be changed at least every 90 days.

• All production system-level passwords must be part of the Information Security administrated global password management database.

• All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days and cannot be reused, as far back as the past 3 passwords.

• User accounts with access to company systems must have a unique password from all other accounts held by that user.

• Passwords must not ever be inserted into email messages or other forms of electronic communication.

• All user-level, system-level access level passwords must conform to the guidelines described below:

Guidelines - Password Construction Requirements

i. Be a minimum length of eight (8) characters on all systems.

ii. Not be a dictionary word or proper name.

iii. Not be the same as the User ID.

iv. Expire within a maximum of 90 calendar days.

v. Not be identical to the previous three (3) passwords.

vi. Not be transmitted in the clear or plaintext outside the secure location.

vii. Not be displayed when entered.

viii. Ensure passwords are only reset for authorized user.

Password Deletion

All passwords that are no longer needed must be deleted or disabled immediately. This includes, but is not limited to, the following:

When a user retires, quits, is reassigned, released, dismissed, etc. :

• Default passwords shall be changed immediately on all equipment.

• Employee should notify his or her immediate supervisor.

• Agent should inform his or her point-of-contact (POC).

• Supervisor or POC should fill out a password deletion form and send it to their company POC

• Their company POC will then take the necessary steps and actions to delete the user's password and delete or suspend the user's account.

• A second individual from that department will check to ensure that the password has been deleted and user account was deleted or suspended.

• The password deletion form will be filed in a secure filing system, soon to be moved to CertainSafe.

Password Protection Standards

Do not use your User ID as your password.

Do not share ANY passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential company information.

List of "do not's"

• Don't reveal a password over the phone to anyone

• Don't reveal a password in any email message

• Don't reveal a password to the boss

• Don' talk about a password in front of others

• Don't hint at the format of a password (e.g., "my family name")

• Don't reveal a password on questionnaires or security forms

• Don't share a password with family members

• Don't reveal a password to a co-worker while on vacation

• Don't use the "Remember Password" feature of applications

• Don't write passwords down and store them anywhere in your office.

• Don't store passwords in a file on ANY computer system other than CertainSafe.

If someone demands a password, refer them to this document or have them call the Executive Vice President of the company. If an account or password is suspected to have been compromised, report the incident to the Executive Vice President of the company and change all passwords as a precaution.

Password cracking or guessing may be performed on a periodic or random basis by management. If a password is guessed or cracked during one of these scans, the user will be required to change it.

Disposal of Personal Information

WORLDWIDE INFORMATION is committed to the proper disposal of personal information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal. WORLDWIDE INFORMATION requires the pulverizing or shredding of papers containing personal information so that the information cannot practicably be read or reconstructed, and the destruction or erasure of electronic media containing personal information so that the information cannot practicably be read or reconstructed. We only allow approved personnel access to this internal confidential information.

Use of one of the provided CPS710 UNCLASSIFIED hard copy paper containers is mandatory for the disposal of documents that are anything more than genial waste. Should there be a document that is questionable as to its' content, the CPS710 shall be used.

Monitoring regarding Certain Services

WORLDWIDE INFORMATION may from time to time monitor compliance with established standards by subscribers, clients, as well as Researchers, whom interface with certain WORLDWIDE INFORMATION services, to ensure that certain information is being used is only for permissible purposes allowed under the relevant agreement for service being provided and is done so in a complaint manor.

WORLDWIDE INFORMATION may immediately cease providing all or any such services to any subscriber, clients, as well as Researchers that are not in full compliance with the preceding as well as applicable laws and standards. WORLDWIDE INFORMATION or certain business allies may also conduct periodic compliance audits or to review an appropriate sample of authorizations, as well as to confirm relevant consent(s). Certain data or services may not be provided to the relevant subscriber, clients, as well as Researchers in the event of non-compliance with the preceding.

Due Diligence Regarding Certain Services

To ensure that certain data is safeguarded and only provided to companies/approved users that have been appropriately verified and credentialed, WORLDWIDE INFORMATION may undertake due diligence on any subscriber of relevant services prior to granting access to such information. Such due diligence may include credit reports. If a credit report is not available or consent to access a credit report is not provided, certain data or services may not be provided to the relevant subscriber/user. In addition, WORLDWIDE INFORMATION will require a subscriber client, as well as Researchers to sign a service agreement prior to certain services being provided.

Security Utilizing/Matching Certain Numbers

In order to protect sensitive data from the risk of identity theft and other possible fraud, WORLDWIDE INFORMATION may insist that clients facilitate the matching (for verification purposes) of certain numbers or partial numbers which are personal to the client, and relevant services may only be delivered upon relevant matches occurring.

Security Training

All employees must go through the company provided security training mandated by management and attend regularly scheduled update meetings as required. Each employee must attend a minimum of (1) security refresher session per calendar year. Additionally, all employees are required to read the Security /Privacy Policy, understand it, use training they receive for their specific job roles, and sign the Security Policy

Physical Security

Access Procedures

Pre-approval must be provided by Executive Management prior to any employee receiving "Key" access to facilities. Any time an employee is grated key access, HR must be notified so they may keep track of those with facility accessibility and in the case of termination. All confidential, sensitive and or valuable information, must remain secured with access only to those who use the items. Entrances to our offices must be kept locked on the outside to prevent people who don't work at our facility from entering. In the extraordinarily "rare" event of a customer visit, the visitor must provide identification if unknown by the company, and in either case, be personally escorted at all times until their departure.

Security System

The company alarm system must be armed at any time there are no employees present within the facility. The alarm system is centrally monitored and shall have a panic option, just in case it should be necessary. The alarm system additionally has cameras in some areas so employees at times will be monitored on video. Only those employees with "Key" access shall be granted alarm code access. No two employees shall share a single code.

Vulnerability Scans on System Networks

Vulnerability Scans on System Intranet Networks shall be performed on a minimum of a quarterly basis by company identified IT staff or by third party vendor. On stationary desktops as well as laptop computers, all antivirus software as well as Windows updates shall be verified. All firewalls,

Must be both tested and verified regarding their ability to function as designed. Any errors, corrections or hardware updates necessary shall be performed to ensure proper security on the company's IT infrastructure.

E-mail

We view E-mail as not a secure medium for sensitive data transmission and insist that appropriate precautions be taken when we are contacting others, or others are contacting us to send personal or confidential information. We will NEVER ask for "Credit Card" payment information, NPI or PII information via email, so please do not ever send it to us via email delivery.

Correcting and Accessing Personal Information

You are entitled to ensure that personally identifiable information in our file is correct and current. You may review this information by contacting us or by using the methods listed on our website.

An individual may ask for access to personal information we hold about him or her at any time.

Detailed requests which require archive or other retrieval costs may be subject to our reasonable fees and disbursements (including any actual out-of-pocket expenses).

An individual's rights to access his or her personal information are not absolute. There are several situations where we may deny access. If we deny your request for access to, or refuse a request to correct personal information, we will provide a reason or reasons for doing so.

Web Site

Our website may contain links to other sites, which are not governed by this Policy.

On our website, like most other commercial websites, we monitor traffic patterns, site usage and related site information to optimize our web service. We may provide aggregated information to third parties, but these statistics do not include any identifiable personal information.

When you visit our website, we may track information to administer the site and analyze its usage. The following are a few examples of information we may track: your Internet protocol address; the kind of browser or computer you use; the number of links you click within the site; the Province, state, county, or jurisdiction from which you accessed the site; the date and time of your visit; the name of your Internet service provider; the web page you linked to our site from; pages you viewed on our site, and how long you visited for.

In some cases, we may use cookies to personalize or enhance your user experience. One of the primary purposes of cookies is to provide a convenience feature to save you time. Hence, this simplifies the process of delivering relevant content and eases site navigation by providing and saving your preferences and login information as well as providing personalized functionality.

You have the ability to accept or decline cookies. Most web browsers automatically accept cookies, but you can usually modify your browser setting to decline cookies. If you should decide to reject cookies by changing your browser settings, then be aware that this may disable some of the functionality on our website.

Constituent Change of Status

Once a termination decision has been made by the immediate supervisor, management must conduct an exit interview. It is important that the reasons for the employee's discharge are explained during this meeting. The explanation should be candid and concise, in accordance with all available evidence, and consistent with any explanation of the termination that will be provided to the employee. The employee must be advised and be reminded of any covenants not to compete and of the employee's continuing obligation to protect the company's trade secrets.

The employee’s supervisor is required to complete the company’s comprehensive release and termination document. It must be provided to the employee for signature and a request must be made for them to sign the document. If the employee refuses to sign, notations must be made to reflect the refusal.

In some cases, a supervisor may not want the employee to remain on the premises for any period after the termination notice is given (e.g., where there is a concern regarding possible vandalism or sabotage of company equipment) or may not even want the termination interview conducted on company property (e.g., fear of violence). In these instances, thought should be given to terminating the employee by telephone or by letter.

Once notice has been given, all efforts must be made to prohibit the use of company property. The written notice of dismissal and order to leave the workplace should also advise the employee that he or she is not to take any company property with him or her and that he or she is not to make any personal, unauthorized use of company property, such as telephones for long-distance calls or the photocopy machine. If necessary, notify the former employee that the police may be called. The written notice should further advise the employee that if he or she is not gone by the deadline, police and or security officers will be called to escort him or her from the premises.

Do not touch the departing person. If it becomes necessary to have security personnel physically escort the employee out, it is very important that they be able to do this peaceably. If it appears that the dismissed employee will leave only under escort, it may be wise to clear the immediate area of all other personnel.

Ensure that prior to the employee departure, ANY AND ALL COMPANY PROPERTY is properly accounted for and collected. Ensure that "IT" has been notified and that all security credentials have been removed so that access to systems has been eliminated. Change locks, if necessary. Once the employee leaves the office or building, as he or she must sooner or later, he or she should be prevented from re-entering. The disruption caused by a dismissed employee's temporary refusal to leave is a lesser evil than the liability that can attach as a result of any physical force used on the employee, especially if coworkers are present to observe it. Supervisors should consult HR for assistance in this process.

Changes to this Privacy and Security Policy

WORLDWIDE INFORMATION, LLC reviews all its policies and procedures periodically. We reserve the right to change this Privacy and Security Policy from time to time without notice

Approved by Steven R. Russo

Executive Vice President for distribution and use

Requests for Access

Any questions or any access requests regarding personal information should be directed to the professional with whom individuals normally deal in writing, and forwarded onto our Chief Technology Officer at:

Chief Technology Officer
Worldwide Information LLC
100 Cummings Ctr Ste 331A
Beverly, MA 01915

by email to Support@worldwideinformation.com by phone to (978) 712-2001 x 233

Access to any company systems containing PII and or personal information shall be on a "need to have" basis. Only those staff members requiring access to specific areas of work that they perform shall be granted access to those areas in which they require to perform their job responsibilities accurately and efficiently. This includes both physical as well as electronic access.

At any time, an employees' role changes, their access to systems shall be reviewed by their supervisor in order to ensure their access is properly controlled.

End of Policy