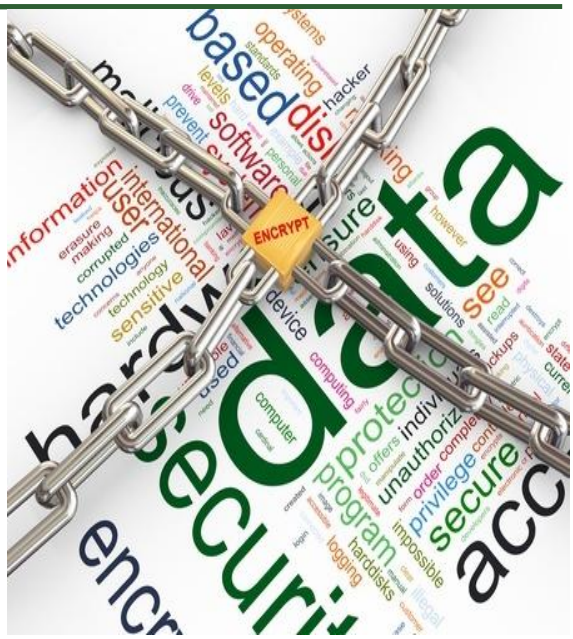
HR ProFile Employment Screening

Data Security & Protection



Data Security/Protection Policy

Users in-house at the HRP secured facility are all controlled by non-disclosure/confidentiality agreements with regard to information technology and company equipment (in addition to all other elements of the business), and are also only given information needed to complete their specific jobs or categories of work on-site. On-board training begins with a company orientation session to convey the standards of behavior, importance of work we perform, and confidentiality of data we handle.

In-House Production

None of HRP's internal operations are outsourced including information systems and accounting (with the exception of payroll, which is domestically outsourced). All employment screening products and services are produced and/or compiled at this location. More specifically, order entry, phone verifications, report typing, product transmission, information systems, programming, and accounting are all performed by HRP staff members. All documents are scanned into an in-house document management system. All paper copies are disposed with a professional on-site shredding service. No personal information is conveyed over the phone except to person(s) with correct credentials.

Website Access & Passwords

Access to the secure website is available only to authorized personnel designated by our clients. Logins and passwords can only be issued via phone after positive identification of the authorized caller. Login passwords are stored in encryption form to avoid "hacker" access to such information. Information on the website is filtered in accordance with the username plus password access key. Any unauthorized attempts to retrieve information are railroaded to a benign area of the website.

Employee Separation Procedures

Separation of employment from HRP by any employee is dealt with in three phases:

1) Employee's password-based accounts are deleted or locked with a proprietary security algorithm that is not known to anyone but IT infrastructure and management staff.
2) All separated employee data is copied from their former interface (computer) and archived for later possible retrieval of missing information or tracking/reference purposes.
3) The employee's interface is re-commissioned for use by a future employee or purpose after removal of all former employee's archived data.

Data

Except for the Director of Information Systems, no data is taken off-site for use on any company or personal computers by employees. Any 3rd-party company that is doing business with HRP is contractually bound to non-disclosure/confidentiality agreements as well as data nature and purpose

restrictions. No personal applicant-related data is exchanged between HRP and its clients/vendors without an encryption protocol or point-to-point secure exchange. No HRP data is treated as public for insecure transmission or reception.

Information Technology

HR ProFile's IT infrastructure employs redundant backup systems with periodic data snapshots (direct byte-mapping copies) of active data are performed once per hour for minimal loss in the rare case of system malfunction. All server-based data is backed up on a whole-disk basis once per day in a two-phase copy; the backup is stored on removable drives that are swapped out, then taken off HRP premises by authorized personnel.

HRP servers are fault-tolerant in the case of individual server component hardware failure. No individuals (other than network administrators) -within or with any relationship to HRP - have access to the servers' administrative-level access or logins. Services used on-site for file sharing and data entry, manipulation, and extraction are locked to valid data points and user / group permissions for accessibility.

The network topology is as secure as possible. The HRP network consists of dedicated telecommunication equipment and protection from attacks. HRP's extranet telecommunication provider is the one with the highest number of years of operation and service provision in the entire area. Contracts for minimized down-time (even in the event of a disaster) are in place. The HRP network consists of a drill-down from top-to-bottom as follows: Extranet → Router/Firewall, → (DMZ) → Intranet. Web-based services reside in the DMZ and are restricted to only the web service ports – 443 (secure) and 80 (redirect-only). The secure web server employs TLS1.0 encryption. The web server logical entry points are programmed in PHP with regard to restricted requests and validation of return results to ensure security. HRP's internal databases can only be accessed by the web server through the DMZ, in reverse, with limited secure table access restriction. Data feeds from clients and external service providers can only be placed in a secure FTP location (with firewall and encrypted, security-based restriction), where internal scripts reverse-pull them from the DMZ and process them with strict validation and processing before entry into the internal database or any other portion of the server infrastructure. The HRP off-site, public web site contains no sensitive data or points of access to the secure server other than a manual click to redirect for client purposes only.

HRP's other services (such as outbound email notifications and internal system-based email) are port-mapped from the firewall directly to the internal server that hosts this service. Only the services in question are used on the servers mentioned in this paragraph, and they are only used-service oriented, with only the ports singularly used for those services forwarded to the specific server's address. Incoming connections are not forwarded to any specific servers on an external-to-internal IP basis (all are port-related only).

Usage of secure remote management (Secure Shell – SSH) is directed only to the DMZ server. The DMZ server internally prohibits connections from an IP address after three (3) connection attempt failures. This is not account-based, but rather address-based for maximized security against potential "hackers."

HRP telecommunication (data and voice) is guaranteed under a Service Level Agreement (with 2 hour turn) by the provider unless a major disaster or unusual outage occurs. If such an event does occur, the provider guarantees business service restoration, with backup generators on-hand, as quickly as possible. HRP's external off-site public hosting provider also maintains backup generators for emergency power. If local power is not restored in a timely fashion by the energy provider, HRP maintains an on-site backup power generator, as well as uninterrupted power supplies for server health. For local power, HRP's

campus resides on the Emergency line of the grid, ensuring no disruption due to forced brown-outs, and first in order of return-to-service.

All system and service-oriented log files on each of the servers are inspected on a daily basis to detect any anomalies that may point to security risks or possible failures. HR ProFile manages external-to-internal system security based on the following:

- Restriction by IP address, subnet, or domain
- Restriction by usernames and passwords
- Encryption using public/private key cryptography

HR ProFile has never suffered any breaches, thefts, or lost client data. In the event of an improbable security breach where sensitive information has left the HRP premises in any fashion, clients and individuals will be contacted directly and will be assisted in whatever means necessary (within the limits of our liability) to recoup any losses. Legal security breach documents are in place and will be directed toward those that may be affected, available for individual or mass-mailing, depending on the specific circumstance.

Privacy Policy

The Website.

HRProfile.com is a Website owned and operated by HR ProFile, Inc., an Ohio corporation located at 8506 Beechmont Avenue, Cincinnati, Ohio 45255 ("HRProfile.com"). HRProfile.com respects your privacy and has written this Privacy Policy so that you are aware of the information HRProfile.com collects from you and how the information is used. Sections 13 and 14 apply specifically to data collected pursuant to the performance of certain investigative services for clients (which is not collected through this Website), while the remainder of the provisions apply to data collected pursuant to use of the Website.

Eligible Users

Use of the Website is governed by the laws of the United States. When you provide us with information, you acknowledge that the information will be stored and processed on servers located in the United States. No one under the age of 18 may use the Website. This Website does not comply with the terms and conditions of the Children's Online Privacy Protection Act.

Information Collected By Us

You may access and use the Website without completing a user registration and without providing us with your Personal Information. "Personal Information" means information that identifies a person, such as the person's full name, business address, email address, telephone number, or any other information that would allow someone to identify or contact you. If you wish to receive more information about our products and services or sign up for our newsletters and other publications, you must provide us with your Personal Information.

Use of Personal Information

We use your Personal Information to communicate with you about our products and services and to provide you with our newsletters and other publications. We generally do not disclose Personal Information to third parties except as necessary to comply with applicable law or to investigate wrongful activity. We may disclose Personal Information to trusted third party contractors who assist us in running the Website and performing services for us. We do not sell Personal Information to third parties for direct marketing purposes.

Use of Cookies

We may place or recognize a unique "cookie" on your browser. A cookie is a piece of data stored on the user's hard drive containing information about the user. We may use cookies to enable us to track and target the interests of our users to enhance your Website experience. Usage of a cookie is in no way linked to any Personal Information while on the Website. If you reject the cookie, you may still use the Website.

Use of Log Files

We may use IP addresses (log files) to analyze trends, administer the Website, track the movement of users, and gather broad demographic information for aggregate use. IP addresses are not linked to Personal Information.

Suspected Privacy Policy Violations

If you feel that HRProfile.com is not abiding by this Privacy Policy, please contact HRProfile.com via registered mail to: HR ProFile, Inc., 8506 Beechmont Ave, Cincinnati, OH 45255, Attention: Privacy Compliance Agent.

Notification of Changes

You should review this Privacy Policy whenever you visit HRProfile.com in order to be aware of the ways that your information is used. HRProfile.com reserves the right to change the Privacy Policy of HRProfile.com at any time. HRProfile.com will post Privacy Policy changes on this document so that HRProfile.com users are always aware of what information HRProfile.com collects, how it is used, and under what circumstances, if any, HRProfile.com discloses it.

Website Links

The Website may contain links to other websites. This Privacy Policy applies solely to information collected by HRProfile.com. HRProfile.com is not responsible for the privacy practices of other websites linked to this Website. HRProfile.com encourages you to read the privacy policies of websites connected through this Website.

Security

The Company does not make warranties or representations regarding the security of Content. While we cannot guarantee the security of information, we utilize a combination of online and offline security technologies, procedures and organizational measures to help safeguard consumer information against loss, misuse, and unauthorized access, disclosure, alteration and destruction. Access to certain HR ProFile web pages and online services is not available to the general public

and requires a login code and password provided by HR ProFile. Those web pages utilize a combination of online and offline security technologies, and the information transferred to and from those pages is made available only to clients of HR ProFile. On these web pages, HR ProFile collects only information that the user voluntarily shares with HR ProFile.

√ Incorporation by Reference; Entire Agreement; Severability

The Terms of Use for HRProfile.com are hereby incorporated by reference and made a part hereof. The Terms of Use and the Privacy Policy constitute the entire agreement between you and HRProfile.com with respect to use of this Website. Should any provision of this Privacy Policy be held invalid, unlawful or for any reason unenforceable, then the invalid, unlawful or unenforceable provision shall be severable from the remaining provisions. Such invalid, unlawful or unenforceable provision shall not affect the validity or enforceability of the remaining provisions.

√ Your California Privacy Rights

HRProfile.com complies with the California Online Privacy Protection Act of 2003, California Business and Professional Code 22575 - 22579. If you are a California resident, we will, upon your written request, provide you with:

a.) The names and addresses of all third parties to which HRProfile.com has disclosed your Personal Information during the preceding year for direct marketing purposes (if any).

b.) The categories of information HRProfile.com disclosed to third parties for direct marketing purposes during the preceding calendar year (if any); and

c.) If the nature of the third party direct marketer's business cannot be reasonably determined by the third party's name, examples of the products or services marketed. In order to obtain this information, please contact us at: HRProfile.com, Attention: California Privacy Rights, HR ProFile, Inc., 8506 Beechmont Ave, Cincinnati, OH 45255. Please include your name and the address where we should send our response. We will attempt to respond within thirty days after receipt.

California Privacy Practices With Respect to Company's Preparation and Processing of Investigative Consumer Reports. Company is subject to California Civil Code Sections 1786-1786.60. In performing investigative services for our clients (which services shall be subject to the terms and conditions of an agreement between Company and our client and not by the Terms of Use for this Website), Company may collect certain personal information (as defined in Section 22577, California Business and Professional Code) about a consumer (the "Consumer Information") and provide such Consumer Information to our client. An individual's Consumer Information may only be collected and disclosed to our client pursuant to a written authorization and for a permissible purpose, as required by the Fair Credit Reporting Act.

a.) Privacy Practices With Respect To Consumer Information Collected in the Preparation and Processing of Investigative Consumer Reports. When HR ProFile conducts a background screening investigation about you, HR ProFile may disclose information that you submit through this web site to the HR ProFile client that ordered a background screening investigation on you. HR ProFile also may disclose your information to certain third parties as necessary to conduct the background investigation (such as educational institutions, prior employers, courts, law enforcement agencies and other persons or entities that may provide or verify information about you), as well as to a third-party representative or subcontractor authorized by HR ProFile to assist in the background screening investigation. These third party representatives and subcontractors include service providers that help host or support

the web site or otherwise provide technical assistance, court researchers and other data and service vendors. HR ProFile transfers to these representatives and subcontractors only the personal information they need to deliver to HR ProFile (for the benefit of HR ProFile's client) the requested product or service. HR ProFile prohibits these third parties from using that information for any other purpose. HR ProFile requires that these parties maintain commercially reasonable measures to protect the confidentiality of your information.

b.) Personal Information Disclosure: United States or Overseas. Personal information submitted to HR ProFile for a background screening investigation may at times be transferred outside of the United States in order to perform the background investigation. All personal information will be transmitted and stored in a secure manner in accordance with the terms of this Privacy Policy.

c.) Contact Information. If a consumer requires assistance regarding Company's privacy practices or policies in the event of a compromise of the consumer's information, he or she may contact the Company as follows:

Contact Name:	Director of Information Systems
Mailing Address:	8506 Beechmont Ave. Cincinnati OH 45255
Email Address:	info@hrprofile.com
Telephone Number	800-969-4300

HR ProFile is a full-service, trusted, industry leader with over 20 years of experience in all areas of Human Capital Management and Employee Screening. We provide Background Checks, Drug Testing, Criminal & Court Checks as well as Reference & Education Verification to clients in all industries Nationally and Internationally. We partner with our clients to ensure best hiring practices and Fair Credit Reporting Act (FCRA) compliance. HR ProFile provides market leading innovations, customized and scalable solutions and pricing, as well as unparalleled personal and professional customer service.