

Describe your company's present privacy policies with respect to the customer and consumer information you receive for employment screening purposes.

HireRight is committed to maintaining stringent data security through our systems and processes to ensure that client data is kept safe and secure. As a Consumer Reporting Agency, data security is a top priority for HireRight at all times, and our concern regarding security is reflected in our policies, technology and our processes. HireRight has adopted the International Standards Organization's 27001 standard as our guideline for continuing to ensure that our security methodology meets globally recognized industry best practices. We conduct regular audits to make certain that we have tight controls in place to minimize the risk of fraudulent acts. We also maintain a data security and privacy officer that leads a team of dedicated IT personnel with extensive training in data privacy measures.

Administrative Security

We have built our entire technology system so that neither customers nor employees can access company or applicant information without three identifiers: a company ID, a valid user name and a complex password. Customers can only view data within their own account, based on information they have provided. In order to receive any information through a background request, they must first have a valid account, adequate permission level and key identifying information regarding the individual being screened. A given customer would never have access to another customer's background reports.

Technical Security

Our production systems are hosted externally at SBC Platinum data centers (primary systems in Irvine, CA and complete mirrored back-up systems in Dallas, TX). These centers feature bio-metric access, class 4 environmental controls and are guarded and managed 24 hours a day, 7 days a week, 365 days a year. We maintain sophisticated in-house tracking mechanisms to measure uptime, capacity and performance of all facets of our production systems. We maintain separate development and staging environments to ensure that all software releases are fully tested in an identical environment to our production environment prior to being launched to our customers. In addition, we perform automatic daily data backups. We also maintain a comprehensive business continuity plan, which can be provided upon request.

We employ SSL data encryption when data is transmitted over the Internet, and have installed robust firewalls to prevent external "hacking" into our system. In order to test system security, we have contacted with a third party specialist to routinely audit, review and test our system's security, which includes attempts to gain unwarranted access to our system.

Some additional security measures include the following:

- Automatic daily data back-up
- SSL data encryption
- Stateful firewalls
- Built-in redundancy
- Unique login and complex password requirements for recruiters and applicants
- Centralized system patching/update tools (Redhat Up2Date Network)

Customer Account Security

HireRight has a very comprehensive and thorough data protection policy. The data we collect on behalf of our customers and partners is their data and it is our responsibility as a service provider to ensure the protection of that data. Our customers' data is never used for any purpose other than for the processing of

requested products from HireRight. The data is never sold, viewed, distributed in any means or reused in any manner other than as intended by the customer or partner.

Clients can create permission levels for their individual users, including the following: the services a user can order, whether a user can view the results (and at what level of detail), whether a user can view the details of another user's applicants, ordering budgets, access to international ordering, the ability to adjudicate results, and many other features. As additional protection of sensitive information, SSNs are masked in applicant list views, billing and e-mail communications.

Candidate's information is stored in HireRight's system, which features the most advanced security, including external Web hosting. Our leading edge Web-hosting provider features data centers in a dedicated, separate, and highly secure environment. These centers are monitored and managed 24 hours a day, 7 days a week, 365 days a year.

Complex Passwords

Managers will have access to create and manage user passwords on an ongoing basis. All password access is through secured means. Our customers access their accounts and reports through secured https://www sessions using 128-bit encryption. Our internal HireRight passwords are changed every 90 or 180 days depending on the type of system and access provided. We use a complex password scheme and have had our systems tested externally to ensure our own compliance in using complex passwords. We require our customers to change their account passwords every 30 to 120 days. All reports on the Management Reporting system dynamically and automatically mask sensitive personal information according to the California SB 1386 Disclosure law.

Encryption

HireRight has invested heavily in encryption technologies. HireRight encrypts sensitive data transmission over the Internet with 128bit SSL. Data between the HireRight application server and the database server is encrypted with IPSEC encryption; sensitive data is encrypted with 256bit AES encryption before being stored to disks. In addition, HireRight backup tape is encrypted using AES or PGP, depending on operating systems.

Integrations Security

When sensitive personal information is transmitted from an Applicant Tracking System (ATS) to HireRight, it is sent over a secure socket layer using 128-bit encryption. Both the ATS and HireRight must have commercially viable security certificates installed from a verified source. If necessary, HireRight has many other secure data transfer mechanisms and protocols that it can support including PGP encryption and SFTP. HireRight's flexible integration architecture is designed to rapidly integrate with virtually any data form or representation (provided the format is documented) and a variety of transport protocols, including http, https and FTP. Our preferred mechanism for data exchange is XML. HireRight is an active member and contributor to the HR-XML forum and has used consortium standards whenever possible. HireRight has the ability to send and receive data in real-time or via batch uploads/downloads.

HireRight Employee Security

Our emphasis on security is equally reflected in the way we work. All employees and contractors of HireRight receive a thorough background check. Additionally, security training is part of every new employee orientation. We operate in an almost paperless environment, but shred all paper documents to the extent that such are generated. In addition, we have invested in state-of-the-art security equipment in our facilities, and actively monitor and control the entrance of anyone to our premises.

HireRight's certification and training philosophy is to ensure the highest quality employees, security of information and a safe work environment. Every HireRight employee must read and sign a comprehensive HireRight Background Check policy and confidentiality agreement. All employees and contractors of HireRight receive a thorough background check. Additionally, all employees and contractors undergo mandatory security and data privacy training as part of new employee orientation.

Physical Security

HireRight maintains state-of-the-art security equipment in our facilities, and actively monitors and controls the entrance of anyone to our premises. We operate in an almost paperless environment, but shred all paper documents to the extent that such are generated.

NAPBS Founding Member

HireRight is one of the founding members of the National Association of Professional Background Screeners (NAPBS). NAPBS was formed to promote a greater awareness among employers nationwide of the growing importance of conducting background and reference checks. The Association's members are companies from across the country that provide pre-employment/background screening, court records research, and tenant screening services. NAPBS helps develop and coordinate training and other relevant programs to enable its members to better serve their clients, to promote and maintain the highest standards of excellence and ethics in the background screening industry, to ensure compliance with the Fair Credit Reporting Act, and to foster awareness of issues related to consumer protection and privacy rights within the industry.