Confidentiality and Legal Issues of Employee Screening

Pre-employment screening provided by Integrated Screening Partners is completely legal as long as the information is used correctly and the applicant has signed a consent form. Integrated Screening will advise employers on how to use information once they have it. Employers performing background checks with the consent of their applicants place themselves at very little legal risk compared with the legal and financial risk associated with a bad hire.

Information obtained for employment purposes is subject to the requirements of the **Fair Credit Reporting Act (FCRA)**. The FCRA regulations include the following: The company must agree to make a clear and conspicuous written disclosure to the applicant prior to obtaining the report, the company must obtain prior written authorization from the applicant, and the company must not use information obtained to violate any federal or state equal opportunity law or regulation. Prior to taking any adverse action based on the information provided in the consumer report, the company should provide the applicant with a summary of their rights under the FCRA and a copy of the consumer report. ISP will provide you with the necessary documents, such as a consent form and the summary of consumer rights under the FCRA.

The following is excerpted from our Data Privacy and Data Security Policies:

Information Collected

ProMesa Enterprises, Inc. collects personal data provided by our clients for purposes of conducting employment screening only. The data collected includes, but is not necessarily limited to: Full Name, Alias Name(s), Date of Birth, Address History, Employment History, Education History and Social Insurance Number.

Use of Collected Information

ProMesa Enterprises, Inc. does not resell, or in any way share, any of this data with any person, agency, or organization not explicitly named in the consent form signed by the subject except for purposes of conducting the investigative report. Specifically, ProMesa may share certain vital information required by police agencies, education institutions and employers to those agencies for purposes of obtaining information on criminal history, employment and education claims. We may share the personal information gathered with other companies we have hired to provide services for us. These companies, our vendors, are contractually bound to use personal information we share with them only to perform the services we have hired them to provide. We do not share, sell, or lease personal information collected to any third-party for their marketing use. We will release such data only if directed to do so by the subject, if required by law to do so, or in other legally limited circumstances.

Security of Collected Information

Data Security within Promesa is maintained through both physical security and data security. Promesa employs card-reader entry technology at our physical location. At no time is a non-employee granted access to our workspace without the accompaniment of an employee. A central computer that operates the system logs every entry and exit from our physical space. Our data center is secured using the same entry method as the outer perimeter as well as its' other security features. We employ two 5-ton air conditioning units set up redundantly to cool our data center. We also utilize a dry-pipe fire suppression system to be certain that no false alarms or fires in other parts of the building will destroy our servers. Additionally, there is enough battery backup in our data center to ensure that our core servers will run for up to 10 hours in the event of a power outage. Our database server, which holds all data sent to Promesa, has redundant power supplies, redundant gigabit network interface cards, and is set up in a RAID 5 configuration with 5 redundant hard drives.

At the data level, there are a number of steps Promesa has taken to ensure the security of the data. At the helm of our network reside two redundant "SuSE Linux Firewall on CD" deployments. This firewall/router is diskless, that is, it boots from CD and reads the rules from a read-only floppy disk – there is no hard drive. This makes intrusion extremely difficult as there is very little, if anything, for a hacker to exploit. Just past these firewall/routers is our DMZ (de-militarized zone) where our web server resides. The web server utilizes https (128 bit SSL encryption) technology. The web application used to input and output data to and from the database server is password protected. Guarding the internal network is a Cisco 1605 router. This ensures that anything in the DMZ can't infiltrate the internal network. Our database server resides inside the internal network, protecting it from the internet and DMZ. The internal application Promesa utilizes to access and work with the data in our database is also password protected and only authenticated users may open it.

Promesa has an open-ended data retention policy. That is, we will keep the data only as long as required by the client. If no time-period is specified, we will keep the data indefinitely.