

## InstaScreen Security Overview

Security is a high priority and an integral part in the design and development of TazWorks' InstaScreen applicant screening system. Attention is given to high publicity threats such as viruses, denial of service attacks and other malicious activities over the Internet, as well as to maintaining the integrity and confidentiality of sensitive application data such as credit reports, social security numbers, and other identifying information. TazWorks development staff use industry-leading technology to secure InstaScreen and its operating environment, including client authentication (password-controlled access), Secure Sockets Layer (SSL) protocol, 128 bit data encryption, public-private key pair, firewalls, intrusion detection, filtering routers, and data backups. Each component acts as a layer of protection to safeguard information from unauthorized users, deliberate malfeasance, and inadvertent loss.

**Client authentication** – Password-controlled access requires clients to authenticate through a private login ID and password before entering the system. After authenticating to the system, sessions that remain inactive for a period of time are expired, requiring the client to re-authenticate before continuing. Passwords are protected in the system using sophisticated hashing schemes, never shared, and combine with a Secure Sockets Layer (SSL) protocol transport layer to protect against eavesdropping, server impersonation, and stream tampering. Additionally, passwords expire and must be reset every 90 days. The system requires strong passwords that are at least 8 characters in length and that contain at least one each letter and digit.

**Encryption** – All transactions are performed in a secured environment. The client's web browser automatically secures the session with the InstaScreen server by connecting to it using the Secure Sockets Layer (SSL) protocol with 128-bit encryption. The data travels between client and server encrypted and can only be decrypted with a public and private key pair. "Data that is encrypted with the public key can be decrypted only with the private key. Conversely, data encrypted with the private key can be decrypted only with the public key. This asymmetry is the property that makes public key cryptography so useful" (See <http://developer.netscape.com/tech/security/ssl/howitworks.html> ).

**Firewalls, Intrusions Detection and Filtering Routers** – The application server is protected by firewalls, intrusion detection, and filtering routers which verify the source and destination of the request traveling in information packets. The routers and firewalls are configured to reject any unauthorized traffic. The intrusion detection algorithms log every action that comes and goes, to and from our network. The system uses network devices that only allow permitted traffic through the devices. Routers keep out traffic that does not emanate from either end of the secured session between the client and the server.

**Physical Security** – The physical server machines are hosted at a state-of-the-art collocation facility that is staffed on-site 24/7 to provide an immediate response to any incident. Access to the facility is restricted to authorized personnel and is secured by both password-protected keypads and biometric scans. Door, glass, and motion events at the facility are digitally recorded and archived, as well as observed live by facility staff for any suspicious activity. UPS systems and a 500-kilowatt diesel generator ensure electrical service to the facility. Multiple fiber providers provide Internet connectivity with diversified entry points into the facility. The cooling system incorporates redundant components, excess capacity, and high-efficiency technologies to maintain an optimal operating environment for the servers.

**Data Integrity** – Data servers are configured with mirrored hard drives to provide real-time, fail over redundancy. Additionally, nightly backups of data are scheduled, with archives removed weekly to an offsite location for additionally redundancy.

**Client Responsibility** – Clients are expected to guard their password carefully and to not share it with or disclose it to anyone, for any reason. TazWorks staff will never ask a client for their password. Clients must also ensure the security of their InstaScreen sessions, completely logging out of the system when finished and not leaving active sessions unattended. Paper and electronic copies of reports must be carefully controlled to prevent the unauthorized distribution or disclosure of personally identifying applicant information.

A robust and secure system requires a multi-faceted solution with hardware, software, and education. Critical to the success of any secure system is the education of its user community and employees on the importance and sensitivity of information. Knowledge of why and how data is secured, and the permissible uses of all information, is essential in maintaining the integrity of the system and its contents.