Ekeholm and Associates, LLC Security, Assurance, and Compliance

Placing the Emphasis on Securing Your Data

Ekeholm places security of client data as our top priority. With the extreme sensitivity of applicant information we have multiple levels of security in place to ensure the data is never compromised. From the point of transmission, to the storage of your company's data, Ekeholm uses the latest in security tools and practices for your protection. To protect the data from unauthorized access and usage, Ekeholm has several security measures to ensure proper access. The following are some of the levels of security and processes Ekeholm uses to ensure the proper and secure ordering of public records through our solutions.

Physical Security

Our production servers are located in a facility with 24 hour a day monitoring managed by SunGard Availability Services. To control access to the facility, card access and CCTV monitoring systems are used. Personnel requiring access to the data center must be on a pre-authorization list and surrender their valid driver's license prior to being able to proceed into the raised floor area. The servers are located in locked cabinets that can only be access by authorized technology support personnel. Once inside the cabinets, the server console can only be accessed by authorized technical personnel, using IDs with strong type passwords. Under no circumstances do SunGard personnel have access to any client data.

Secure Encrypted Connections

Ekeholm solutions are protected via digital certificates. Certificates are issued by GeoTrust and use 128-bit SSL encryption. GeoTrust's Identity Verification Services ensures the identity of business entities and/or individuals in online transactions. Any connection to the web applications or through the interfaces requires secure socket layer. Users can ensure the information they are sending is protected by locating the lock icon on the bottom right corner of the browser window.

Disaster Recovery

Ekeholm has disaster recovery plans in the event of loss of production servers or the production environment. Business continuity plans outline scenarios and team responsibilities to implement the return of critical operations. Documented plans are tested to ensure decisive results if a scenario should transpire. Agreements and partnerships are in place to provide support and assistance during unfortunate scenarios. Senior management reviews plans quarterly to confirm they are up to date and ensure the entire recovery team understands their responsibilities.

Backups and Reliability

Our production facility is configured to provide redundancy to prevent a single point of failure. All production equipment is covered under service agreements with vendors to ensure optimal turnaround if any hardware failures should occur. Backups are completed on the applications and database to ensure copies are moved off site for storage on a regular basis. Databases transfer all transactional data real time using replication to ensure a secondary server is always up to date. Additionally full, differential, and transaction log backups are completed on our production database servers to ensure every transaction is captured.

Workstation Security

To ensure security a user can only be authenticated into the Ekeholm System from only one workstation at any given time. Users are not allowed to log into multiple workstations with the same valid user account. Additionally an authenticated user is automatically logged out after they are inactive for a specified time period; ensuring terminals are logged out when users leave their machine.

User Authentication

Ekeholm solutions require each user to have a valid username and password. Strong type passwords are enforced to ensure obvious or simple passwords are not selected. Users are also forced to changed passwords every 90 days or risk being locked out of the

system. Only site administrators can reset a user once they are locked out from the system.

Strong Password Support:

- Password must have a minimum length of 8 characters
- Passwords must have at least one number
- Passwords must have at least one lower case letter
- Passwords must have at least one upper case letter
- Passwords must have at least one special or punctuation character
- User name, company names, initials, etc. cannot be included in the password.

Network Security

We use multiple firewalls to ensure only authorized network traffic is allowed. The firewalls log activity and network traffic is monitored by intrusion detection systems to proactively identify security threats. Ekeholm keeps all production databases and EDI connections on a separate private network. The private network is protected with its own firewall and is inaccessible by the public.

Server Security

Production servers are protected with secure access and strong passwords. The number of access points along with the number of authorized users for the servers are limited to ensure security. Operating systems are configured with vendor's latest patches for security purposes.

Data Security

Our databases are located on a separate sub network, which is not connect to the Internet with addresses that are not Internet Routable, A dedicated firewall resides between the applications and databases only allowing data request which originate from set private IP addresses. As an additional layer of security sensitive data is encrypted while at rest in the database. Data is also secured to prevent one customer from accessing another customer's data during each request to the database.

Contract Requirements

All customers using Ekeholm's software as a service solution to order and obtain public records are preauthorized and predefined by contract within our system. The system contract is configured so only authorized services for that particular customer are available. A customer must be authorized to obtain credit reports prior to that service being made available to their contract.

Compliance – Data Availability

Data is accessible on the system for 60 days and is only available to authorized individual users from the requesting client. After 60 days the data is archived and stored on separate media and is not accessible by a client user through the Internet. This archived data can only be retrieved by a special request as a historical view of the original request and must be approved on a case-by-case basis by and administrator. No data is stored for any length of time on the application server.