



Security for the ASEBA Internet Solutions Web-Link, iForms Service, and WebForms Direct

There are five levels of security for ASEBA's Internet solutions. These are **network** security, **application** security, **database and file access** security, **application code** security and **data center** security. These security measures prevent various malicious "attacks", including denial of service, bot infections, cross-site attacks, SQL injections, and deliberate attempts by application users to insert malicious code into ASEBA databases. These security measures also *ensure that data remain private* and help customers to *satisfy requirements of the US Federal Health Insurance Portability and Accountability Act of August 1996 (HIPAA)*.

The security measures overlap and reinforce one another. For example, all access to ASEBA resources requires passwords. Even if this requirement could be bypassed, the data are still encrypted, the no-bot controls still limit the number of repeated access attempts within a time period, and the database is still inoculated against SQL injections.

Network Security

- Encrypted transmission of information between your browser and the ASEBA server
 - We provide communication confidentiality over the Internet using cryptography (2048 bit key) to prevent eavesdropping and packet tampering.
 - We maintain the 128 bit, HTTPS protocol security certificate, published by Equifax Secure Inc., keeping it renewed and current.

Application Security

- Session information
 - A more secure form of the familiar concept of "cookies", session information does not persist after logout. The session information is maintained inside the ASEBA server and is not transmitted to the client browser. Session variables are used for both mundane and sensitive information.
 - Session variables are maintained in the server memory (not on disk) only as long as the user is logged in. When the user logs out of the application or closes the browser the session variables are cleared from memory.
- Password protection
 - Access to the ASEBA applications is restricted to valid account number and password combinations. Do not share your password with anyone!
- CAPTCHA & NoBot controls
 - CAPTCHA is an acronym for "**C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part"
 - These controls must be filled out by people. This prevents denial of service attacks because screen scrapers and other malicious code (bots) cannot interact with the CAPTCHA controls.

Database and File Security

- Password protection
 - This is a database and server access protection that requires a strong password separate from the passwords for regular user accounts. This information is not available outside ASEBA.
- Encryption
 - Identifying data and all deliverable files in ASEBA servers are encrypted using a proprietary private key technology that is account dependent. Unencryption can only be accomplished through the application interface. Unencrypted data and files are re-encrypted by our network security when they are sent to the client browser. Even ASEBA staff cannot unencrypt data and files of customer accounts.
- Redundancy and monitoring
 - ASEBA maintains a separate, off-line, secure database for disaster recovery, redundancy, and backup purposes. Disaster recovery procedures are reviewed regularly.
 - The production database is constantly monitored by remote ASEBA systems to ensure that it is functioning and healthy. Failures to pass health and functioning tests result in immediate alerts to ASEBA staff.
 - The ASEBA servers are constantly monitored by our Internet host provider to ensure that secure access is available at all times to the web application server and database server. Our ISP also provides secure services for database and file backup and recovery.

Code Security

- ASEBA applications are developed using industry standards for code security. These standards are enforced by the code development software. Use of these standards prevents cross site attacks, SQL injection attacks, and malicious database inputs within the applications by users.
- ASEBA applications require valid security tokens for interactions with remote systems. Communications that do not use a valid token are rejected. A token is created during the first transaction in a session and is used throughout that session. The token creation requires the use of our proprietary encryption technology.

Data Center Security

- ASEBA uses a service host and data center provider (Rackspace.com) that surpasses industry standards for physical and virtual security
 - Physical security – The data center is a restricted, locked, environmentally controlled and monitored facility. Redundant and backup electric power and data transmission systems are incorporated into the center.
 - Firewalls – ASEBA uses a hardware and software firewall that allows access to its servers in only very specific ways that are controlled by ASEBA.
 - Controlled Access – ASEBA physically separates the database server from the web applications server. Access to the database is allowed only to the web applications (controlled by session variables and security tokens) and to specific ASEBA computers (controlled by the firewall and passwords).
 - Data backups – The host and ASEBA both provide regular backups of files and databases. ASEBA itself provides remote backups in near real-time of mission critical database tables.
 - Safe Harbor compliance – The host meets European Union privacy and security standards. Their certificate can be viewed [here](#).