



Acesis Security Policies

Overview

This document contains Acesis's security policies. The Acesis security policies provide excellent security for information belonging to Acesis customers, including protected health information (Customer PHI), other Customer Hosted Data and other Customer Confidential Information. For purposes of this document the term "Customer Confidential Information" includes "Customer Hosted Data", and "Customer Hosted Data" includes "Customer PHI".

The policies described below address various administrative, physical and technical safeguards that protect the confidentiality, integrity and availability of physical and electronic information that is generated by, received by or transmitted by Acesis in relation to its customers and its business partners.

1 General Security Controls

- 1.1 Confidentiality Statement. All persons working with Acesis data must sign a confidentiality statement, either as an individual or as an Acesis business partner. The confidentiality statement includes clauses related to general use, security and privacy safeguards, unacceptable use, and enforcement policies. The confidentiality statement must be signed by the party prior to gaining access to "Acesis Confidential Information", including Customer Confidential Information.
- 1.2 Background Check. Acesis performs background checks on all employees who have access to Customer Hosted Data.
- 1.3 Information Security Education and Training. All persons that access Customer Confidential Information receive appropriate information security training along with regular updates.
- 1.4 Disciplinary Process. Formal disciplinary processes are deployed for Acesis employees who violate organizational security policies and procedures. Acesis agreements with its business partners also contain this provision.
- 1.5 Physical and Environmental Security. Physical and environmental safeguards are in place to limit and secure access to Customer Confidential Information.
- 1.6 Workstation/Laptop Encryption. All workstations and laptops that process and/or store Customer Hosted Data use encryption to protect the Customer Hosted Data from unauthorized access. The Acesis application only holds Customer Hosted Data in volatile memory and delivers it from the Acesis server using SSL. No Customer Hosted Data is stored on user laptops by the Acesis application.
- 1.7 Downloaded Information. If Customer Hosted Data is downloaded to a customer's computer via the Acesis platform, the Acesis software ensures that encryption or "blank out" functionality is available for use by the customer.
- 1.8 Removable Media Devices. All electronic files that contain Customer PHI are encrypted when stored on any removable media type device (i.e. USB thumb drives, floppies, CD/DVD, etc.)
- 1.9 Email Security. All emails that include Customer PHI are sent using an encrypted method that is approved by the customer.
- 1.10 Antivirus Software. All workstations and laptops operated by Acesis that process and/or store Customer Confidential Information have a commercial third-party anti-virus software solution in place with a minimum daily automatic update. Acesis production servers that contain or process Customer Hosted Data are totally closed to unauthorized access from external sources.

- 1.11 Patch Management. All workstations, laptops and other systems that process and/or store Customer Confidential Information must have security patches applied.
- 1.12 User ID's and Password Controls. All users are issued a unique user name for accessing Customer Hosted Data. Aceso's policy is that passwords are not to be shared among users. Aceso's password policy can be set up to be customer specific. Customer password policies can be set to specify a minimum number of characters, minimum numbers of different types of characters, password not reusable, and a specified password expiration date. One of the first action items for a new Aceso customer is for the customer to provide Aceso with a description of its desired password policy.
- 1.13 Data Destruction. All Customer Confidential Information is wiped from systems when storage of the Customer Confidential Information is no longer necessary. All Customer Confidential Information on customer-specific removable media is returned to the customer when storage of the Customer Confidential Information is no longer necessary.
- 1.14 Remote Access. Any remote access to customer I.T. environments that involves the display of Customer Hosted Data is executed over an encrypted method approved by the customer. All remote access is limited to minimum necessary and least privilege principles.

2 System Security Controls

- 2.1 System Architecture. The Aceso application is implemented in a multi-tiered Rich-Internet architecture that provides logical separation of the presentation/business logic and database layers. All system requests are authenticated. All system requests to the database layer are made as a trusted sub-system that utilizes a single database access account for all database transactions.
- 2.2 System Timeout. The Aceso application provides an automatic timeout after 20 minutes of inactivity.
- 2.3 Warning Banners. The Aceso application contains a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only. Users of the Aceso application are directed to log off the application if they do not agree with these requirements.
- 2.4 System Logging. The Aceso application logs successes and failures of user authentication when logging onto the Aceso application and when accessing information stored in the Aceso application database. The system also logs all information as supported by the standard Linux Redhat Enterprise operating environment.
- 2.5 Access Controls. The Aceso application uses role based access controls for all user authorization and enforces the principle of least privilege.
- 2.6 Input Controls. The Aceso application does not allow direct database access from client computers. The system does not allow in-line SQL calls from client computers. All user data input is validated before impacting any business logic. The server retains control over all client inputs that are stored to the application database.
- 2.7 Transmission Encryption. All data transmissions are encrypted end-to-end using SSL.
- 2.8 Host Based Intrusion Detection. All Aceso servers that are accessible via the Internet use Linux Redhat Enterprise intrusion detection.
- 2.9 Data Network Firewall. Aceso provides software firewalls to limit external network access to Aceso servers.
- 2.10 Wireless Data Network. The Aceso Wireless LAN utilizes WPA/TKIP security. Wireless LAN clients do not have access to sensitive data.
- 2.11 Incident Management Notification. Aceso's incident management procedure includes prompt notification to the customer if a breach of Customer PHI occurs. Detailed incident management procedures are usually described in the BAA between the customer and Aceso in relation to Customer PHI.

3 Audit Controls

- 3.1 System Security Review. All Aceso servers that are involved with processing and/or storing Customer Hosted Data undergo an annual system security review. Reviews include administrative and technical vulnerability assessments.
- 3.2 Log Reviews. Regular log reviews are conducted for all Aceso servers that process and/or store Customer Hosted Data. Logs are only accessible to personnel having unauthorized access. Logs are maintained for at least one year.
- 3.3 Change Control. Change control procedures are in place for all Aceso servers that process and/or store Customer Hosted Data.

4 Business Continuity / Disaster Recovery Controls

- 4.1 Emergency Mode Operation Plan. Aceso and its relevant business partners have plans and procedures in place to enable continuation of critical business processes and protection of Customer Hosted Data in the event of an emergency.
- 4.2 Data Backup Plan. Aceso and its relevant business partners have plans and procedures in place to backup Customer Hosted Data. The plan includes a regular schedule for making daily backups, storing backups offsite, and specifications for the amount of time to restore Customer Hosted Data should it be lost.

5 Paper Document Controls

- 5.1 Supervision of Data. Aceso's policy is that Customer Confidential Information in paper form is not to be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. Customer Confidential Information in paper form is not left unattended at any time in vehicles or planes and is not checked in baggage on commercial airplanes.
- 5.2 Escorting Visitors. Visitors to areas where Customer Confidential Information is contained are escorted, and Customer Confidential Information is kept out of sight while visitors are in the area.
- 5.3 Confidential Destruction: When authorized by the customer, Customer Confidential Information is disposed of through appropriate confidential means, such as shredding and pulverizing.
- 5.4 Transport of Data. Customer PHI that is kept onsite at Aceso is transported to another location only when granted permission to do so by the customer.
- 5.5 Faxing. Generally Aceso does not fax documents containing Customer PHI. In the rare event that a customer requires Aceso to fax a document containing Customer PHI, Aceso includes in the fax cover sheet a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers are verified before sending.
- 5.6 Mailing. Customer PHI is only mailed using secure methods. Disks and other transportable media sent through the mail are encrypted.