

# Axxerion

## Hosting and Security

- Secure facility
- IP filtering
- Anti virus
- Intrusion detection
- Audit trails
- Network redundancy
- Redundant hardware
- Database encryption
- Secure Sockets Layer
- Secure FTP
- Backups
- Disaster recovery site
- Multi-layer security model
- Private hosting options

---

# Axxerion Hosting and Security

Axxerion has a ISAE3402 Type II certification for development and hosting of cloud-based software. This means that appropriate systems and procedures to control risks have been documented, implemented and effectively used according to an independent external auditor. ISAE3402 is an international standard that has replaced SAS 70 as of June 15, 2011. Axxerion hosts its solutions on state of the art and highly secure data centers with ISO27001 and ISO9001 certification.

## Hosting environment

The data centers have fully redundant network, power supply and connection points so that Axxerion can offer a high level of availability of its services and a secure environment. High speed connections are guaranteed by a direct connection to AMS-IX, transatlantic links in Europe and AT&T's Global Internet backbone in the US.

■ **Electricity:** The data centers are connected to multiple electricity networks. This prevents power failure in case of a cable breach or a malfunctioning transformer somewhere in the power grid.

■ **UPS:** Batteries and UPS systems level off voltage changes in the electrical power supplies. Power supply continuity is guaranteed even if the electricity network is down in case of a major disaster.

■ **Backup generators:** Diesel generators ensure continued power supply if the electricity networks are down for a longer period of time. The data centers have their own diesel generators and fuel to be able to work for days.

■ **Datacenter access:** The data centers are guarded 24 hours per day and are only accessible to authorized personnel. The entrance of the data centers are protected through steel gates, concrete poles and raised bars.

■ **Server access:** All areas in the datacenter are protected by card key systems. All servers are stored in locked cages and physical access to the servers requires a chip card and a key.

■ **White list:** Only Axxerion employees registered on a white list have access to the servers. The datacenter checks identification for all persons entering the server areas.

■ **Network redundancy:** The Axxerion servers connect via multiple 1000 Mbit connections to AMS-IX, MCI UUNet, AT&T Global backbone & Versatel networks. The connections run via Cisco 7600 routers.

■ **Hardware redundancy:** Axxerion deploys a cluster of servers with hot failover. In case of a hardware problem a standby server takes over, minimizing any downtime. Firewalls and switches are configured as pairs in high availability mode.

## Network security

Axxerion provides multiple levels of security for accessing the environment and transferring information.

■ **Anti-Virus:** Gateway Anti-Virus and Anti-Spyware in the firewall scan all incoming traffic for Trojans, spyware and viruses. Day one attacks are prevented by using a dynamically updated database of signatures.

■ **Intrusion prevention:** All network traffic is scanned for worms, exploits and malicious attacks. The signature database is dynamically updated as part of the firewall security service subscription.

■ **IP Filtering:** Axxerion can limit the access to the site only to a certain IP pool. This can be provided on a restrictive basis, where certain IPs are blocked, or granting,

where only certain IPs are allowed to connect.

■ **Password management:** Passwords cannot be viewed by anybody including the system administrator. Passwords must have a minimum length, should contain special characters and may not include repetitive characters. The login is automatically disabled after three failed login attempts.

■ **Auto Logoff:** Clients can setup an Auto Logoff feature in Axxerion when the system automatically logs off a user who has been idle for more than a certain amount of time, typically 20 to 30 minutes.

■ **SSL/HTTPS:** The communication between the web browser and the Axxerion server can be encrypted using SSL and the https protocol, with a 1024-bit encryption key. This way you can be assured that data you enter in the web browser is communicated safely to the Axxerion server.

■ **SFTP:** You can transfer data to and from your own FTP server using secure FTP (SFTP). This uses 1024-bit data encryption for transferring confidential information.

■ **Access log:** The servers and the system keep a record of all user logins and access. The system administrator can see who has accessed the system and at what time. When a user has logged in to the system the last access date is displayed so that the user can be informed of any unauthorized access.

## Data security

Axxerion offers a comprehensive and multi-layered security model. Every user is assigned to one or more user groups. The user groups specify the default access, such as 'full', 'view' or 'none'. These permissions can be refined for individual fields, functions, objects or folders.

■ **Groups and roles:** Users can be assigned to one or more user groups that have a default access permission. User groups are structured as a hierarchy so that they can inherit access permissions from their parent group, which ensures consistency and saves time in setting up the security model.

■ **Object type security:** A default access right can be defined for every object type. For example, users that are assigned to the user group 'external users' will never be able to see any information of the object 'employee'.

■ **Field security:** Every object in the system has a number of data fields. Access permissions can be defined separately for each field and user group. When a field is used on several pages the access rights of that field are the same for all pages.

■ **Object security:** The access permissions for an object type can be overridden at the individual object level. For example, if a user has a default 'view' access to documents the access can be set to 'none' for a particular document (as an exception).

■ **Folder access:** When objects are placed in folders the access permission of the folder applies to all objects and folder in that folder. When the access permission of a folder is set to 'none' the folder is not visible to the user.

■ **Function access:** Access rights can be set for every function, such as create, view or delete. When the access right is set to 'none' the button for invoking that function does not appear. Function access can also be used to set the access permissions to the modules for a particular user group.

■ **Workflow access:** Access permissions to fields and functions can be dependent on the status of the workflow. For example, when a document has a status 'published' it is not possible to change the name of the document or delete the document.

■ **Application security:** Some access permissions are directly set by the application based on business logic. These access permissions ensure data integrity and cannot be set by the user. For example, when a document is checked out the check in button is not available to other users.

■ **Database encryption:** Confidential information such as passwords or salaries are stored in the database using 128-bit encryption using Blowfish database security system. This offers added security when somebody tries to connect directly to the database. An extra seeding algorithm

avoids that equal values result in the same encrypted value.

■ **Disk redundancy:** Axxerion servers use a combination of Raid1 and Raid5 disc arrays. The disk arrays provide hot swappable disks in case of hard disk failures. Axxerion disk redundancy provides data safety without service interruption and without any data loss.

■ **Audit trail:** For any object you can see the history of who has created and last modified an object and at what time. Optionally you can turn on the audit trail for each individual object field, such as the price of an asset or the address of an organization.

## Backup

Axxerion has extensive backup, archiving and storage services.

■ **Live backup environment:** Axxerion provides a fully functional backup datacenter at a different geographical location. The production data is copied every night using secure FTP. Users can access the backup environment to verify the nightly backup. The backup environment also serves as a disaster recovery site in case of a major calamity.

■ **On demand data dumps:** Axxerion allows you to define reports and save the report to a CSV file that you can store in your own environment or import in another system.

■ **Scheduled data dumps:** You can set up a scheduled task where data is extracted based on your own filter criteria and then sent to your FTP server or email address.

■ **Daily database backup:** Axxerion provides a nightly full 'live' backup of all production data. Your nightly backups are available online completely functioning as a live copy of the previous day's information and status.

■ **Monthly database backups:** Axxerion creates a full one month rolling daily backup of all information and programs. A backup of the first day of every month is retained.

■ **Archive DVD:** Clients can order a DVDs with all documents, data backup in XML and CSV formats and all reports in HTML format.

## Hosting options

The most common hosting option is where Axxerion host the environment in a facility that is shared with other Axxerion users. It is also possible to host the environment at another data center or at the client site.

■ **Shared hosting:** Your environment is hosted on servers shared by other users. This is the most economical option and there is no need to buy and configure hardware and software. There is no installation and you can be up and running in a matter of few minutes.

■ **Dedicated hosting:** Axxerion can be hosted in a datacenter of a client's choice. In this option, the client specifies the security provisions of the datacenter and Axxerion works with the client and their choice of the datacenter for hosting the system. Axxerion or its partners can take care of maintenance of the environment.

■ **Self hosting:** Client may decide to host Axxerion in-house. Axxerion system is very flexible and supports different databases and server types. The specifications and information for in-house hosting are available from Axxerion.

Axxerion offers a migration path from shared hosting to dedicated or self hosting, so that you can start quickly and move the environment to a private datacenter at a later stage.

**Axxerion B.V.**  
High Tech Campus 9  
5656 AE Eindhoven  
The Netherlands  
Email: [info@axxerion.com](mailto:info@axxerion.com)  
Web: [www.axxerion.com](http://www.axxerion.com)

**Axxerion Facility Services**  
Ressenerbroek 26b  
6666 MR Heteren  
The Netherlands  
Email: [info@axxerionfs.nl](mailto:info@axxerionfs.nl)  
Web: [www.axxerionfs.nl](http://www.axxerionfs.nl)

**Axxerion USA**  
48 Chula Vista drive  
US-CA 94901 San Rafael  
USA  
Email: [info@axxerionusa.com](mailto:info@axxerionusa.com)  
Web: [www.axxerionusa.com](http://www.axxerionusa.com)