SECURITY HANDBOOK

INTRODUCTION

In this document you will find information about the security policies that Axy7 implements.
Entirely focused on guaranteeing our customer trust on every service Axy7 gives, we have established and followed security policies to complement the existing security layers that Salesforce offers.
AXY7 products are Salesforce add-ons, and they can only work within the user browser in the Salesforce context. Therefore, all of the security protections provided by Salesforce are automatically inherited by our products.

SECURITY OVERVIEW

We work based in the three pillars of applications development:

- Confidentiality: Prevent the disclosure of information to unauthorized individuals or systems.
- Integrity: Maintain and assure the accuracy and consistency of data over its entire lifecycle.
- Availability: Ensure the information is available when needed.

Axy7 is committed to these principles. Providing a security and privacy program that considers security and data protection across our processes.

COMMITMENT ON SECURITY

In Axy7 our employees follow a strict security, privacy, and compliance training that is recurrently reviewed and updated following the Salesforce practices for security. Also there is staff to ensure the protection of company and customer data.

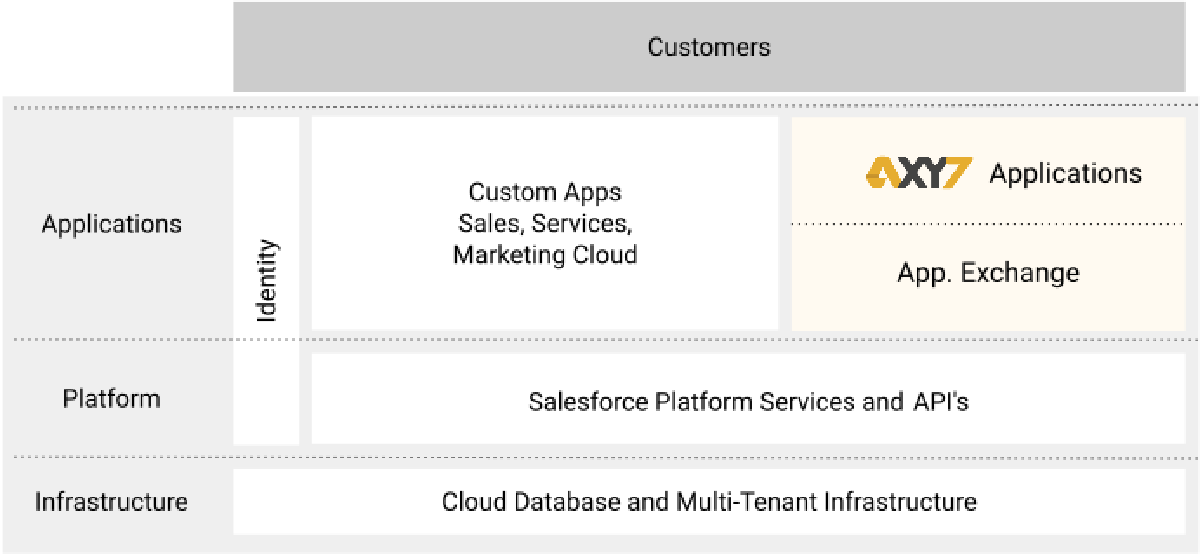
The AXY7 security responsable maintains a constant protocol tracking to ensure our lifecycle process keeps within the security norms.
AXY7 processes and tooling are regularly audited to ensure we meet industry latest standards.

SALESFORCE ®

Salesforce is the most trusted customer relationship management (CRM) platform in the world. In order to be a **certified Salesforce ISV** (Independent Software Vendor) company strict partnership requirements should be complied, including periodic security reviews.

salesforce registered ISV partner

Security Sharing Responsibility Model



Customers

They are responsible for security and compliance of their data in the cloud (e.g.: Manage user access and authorization, configuration of Salesforce platform and backup of data if required)

Axy7

Axy7 is responsible for security of its applications on the Salesforce platform (e.g.: Application security, change management, incident management)

Salesforce

Salesforce is responsible for security of cloud infrastructure and platform. (e.g.: Operate, manage and control host systems, security of underlying platforms and databases, physical security of data centers, audits and certifications of Salesforce platform)

BUILT ON SALESFORCE PLATFORM

ISV

As an ISV, rigorous security standards should be successfully passed every year. This shows the level of commitment on security that Axy7 had, has and will continue having to deliver Trust to our customers.

Security Review Certification

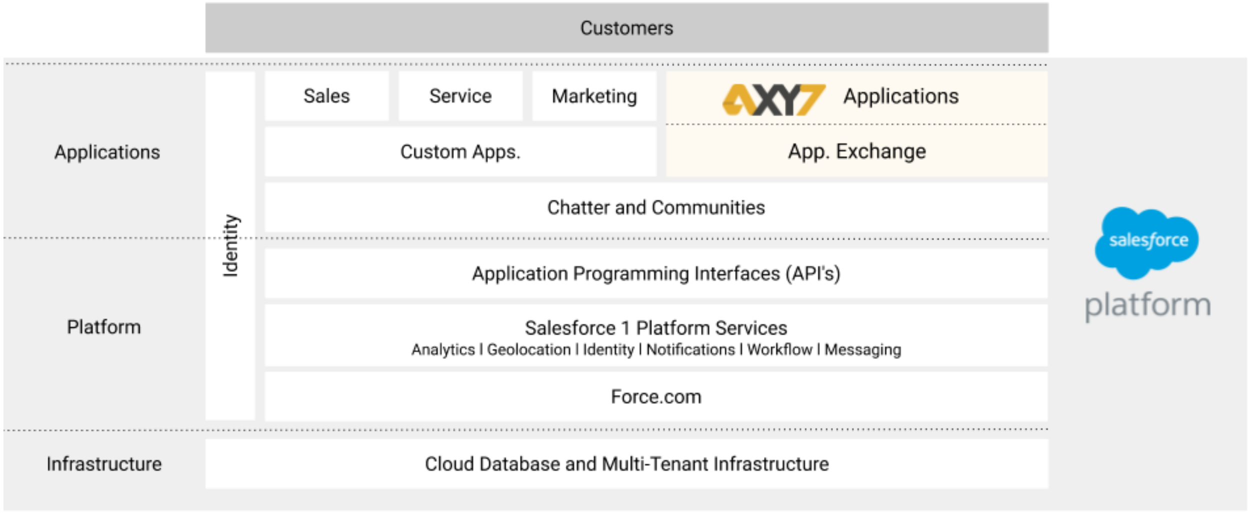
Our applications are submitted to Salesforce as part of the AppExchange Security Review process. Salesforce provides the **AppExchange Security Review program** to assess the security posture of ISV applications published on the AppExchange against industry best practices for Security.
Salesforce commits his security department to scan and review in deep every single component of our products to ensure the security of them.
The security review content extends and cover several layers of security. One example of the coverage is the OWASP pentest.
More information about security review performed by Salesforce.

Trust

Trust is Salesforce number one value and we are committed to follow that value. We understand that security, availability and integrity are critical for our customers.
Since our applications are built 100% natively on the Salesforce platform, Salesforce security is critical to our operations.

Salesforce Platform and Security References

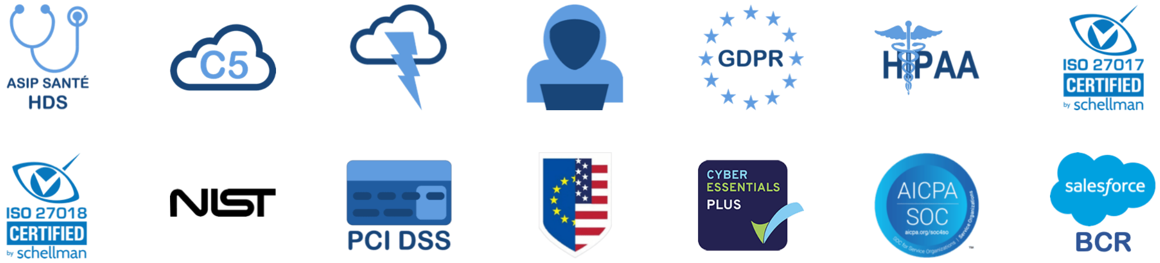
Founded in 1999, Salesforce is an enterprise cloud computing company. Using Salesforce's social and mobile technologies, companies can connect with customers, partners, and employees in entirely new ways. Based on Salesforce's real-time, multitenant architecture, the company's platform and apps give customers the tools to create a social front office and revolutionize the way they sell, service, market, collaborate, work, and innovate.


Customers
Applications
Sales
Service
Marketing
AXY7 Applications
Custom Apps.
App. Exchange
Chatter and Communities
Identity
Platform
Application Programming Interfaces (API's)
Salesforce 1 Platform Services
Analytics I Geolocation I Identity I Notifications I Workflow I Messaging
Force.com
Infrastructure
Cloud Database and Multi-Tenant Infrastructure
salesforce
platform

Axy7 apps are built on Salesforce, means Axy7 apps inherit Salesforce innovations like mobile access, advanced analytics, and the ability to run business in multiple currencies and languages. With an intuitive user interface and flexible architecture, Salesforce drives application adoption, productivity, and security through your organization.

Certifications, Standards and Regulations

As mentioned before, Axy7 Applications run within the Salesforce Platform that cover currently this certifications.



More information about [Salesforce compliance here]()

SHARED AND PERMISSION MODEL

Permission Sets defined

Axy controls CRUD/FLS following Salesforce standards by Permission Sets.
The permission levels manage by default are for:

- Administrator
- C-Level User
- Standard User

This permission structure contains for each application an specific configuration for each Object and field the application contains.

Having said that, Axy applications are easily configurable to adjust the customer needs on visibility and data access from their users.

What is a Salesforce permission set:
A permission set is a collection of settings and permissions that give users access to various tools and functions. The settings and permissions in permission sets are also found in profiles, but permission sets extend users' functional access without changing their profiles.
Users can have only one profile but, depending on the Salesforce edition, they can have multiple permission sets. In order to adjust for your company needs, you can assign permission sets to various types of users, regardless of their profiles.

More information about Salesforce Permission Sets

CRUD/FLS enforcement

Object-level security within the salesforce.com environment is referred to as Create-Read-Update-Delete (CRUD) access. CRUD settings are applied at the profile level and can be used to restrict the actions that users can take on each type of standard and custom object. Field-level security (FLS) is configured similarly to CRUD but allows administrators to define the profiles that can see and write to most fields of standard and custom objects.

More information about Salesforce CRUD/FLS enforcement

Sharing Model

Axy uses OWD (Organization-Wide Sharing Defaults). With OWD you can define the default access level for an object's records with organization-wide sharing settings. Organization-wide sharing settings can be set separately for custom objects and many standard objects, including assets, campaigns, cases, and accounts and their contracts. For most objects, organization-wide sharing settings can be set to Private, Public Read Only, or Public Read/Write. In environments where the organization-wide sharing setting for an object is Private or Public Read Only, an admin can grant users additional access to records by setting up a role hierarchy or defining sharing rules.
Axy7 applications are mostly built using private objects and the record visibility is handled by the Owner and a hierarchy role tree.
Our applications also contain in the setup the option to select with Public Group use for managing sharing to "All Internal Users".

More information about Salesforce OWD Sharing Model

SALESFORCE SECURITY FEATURES

OAuth/SSO

OAuth is an open protocol that authorizes a client application to access data from a protected resource through the exchange of tokens. OAuth tokens are essentially permissions given to a client application. The resource server can validate the tokens and allow the client application access to the defined protected resources. In Salesforce, you can use OAuth authorization to approve a client application's access to your org's protected resources.

2FA

Two-factor authentication is the most effective way to protect your org's user accounts. As a Salesforce admin, amplify your org's security by requiring a second level of authentication for every user login. You can also require two-factor authentication when a user meets certain criteria, such as attempting to view reports or access a connected app.
- Available in: both Salesforce Classic (not available in all orgs) and Lightning Experience
- Available in: Essentials, Group, Professional, Enterprise, Performance, Unlimited, Developer, and Contact Manager Editions

Two-factor authentication is an essential user authentication method—so essential that Salesforce provides two types of two-factor authentication.
Service-based—Also known as device activation, service-based two-factor authentication is automatically enabled for all orgs.
Policy-based—Admins enable policy-based two-factor authentication. It is an admin's best tool to protect org user accounts.
For help with configuring two-factor authentication, see the Admin Guide to Two-Factor Authentication and the Trailhead Module Secure Your Users' Identity.
More information about Salesforce Security Guide here

PRODUCT SECURITY

Application control

Axy7 provides rigorous application controls that ensure you have comprehensive audit trails that can be extended by implementing field history tracking, and cannot subsequently be modified via "back door" manipulation of object data.
In addition Salesforce Shield adds an additional audit layer of data accessing and data edition.
These application controls include:
- Comprehensive audit trails for transactions, master data modifications and security setup changes.
- Segregation of duties.

- Highly granular control of company, object, record and field level access by role.

Disaster Recovery

Because AXY7 applications are 100% Force.com-native, all data processed resides on the Salesforce cloud platform owned, operated and managed by Salesforce. Production data centers are designed to mitigate the risk of single points of failure and provide a resilient environment to support service continuity and performance. The Covered Services utilize secondary facilities that are geographically diverse from their primary data centers, along with required hardware, software, and Internet connectivity, in the event Salesforce production facilities at the primary data centers were to be rendered unavailable. Salesforce has disaster recovery plans in place and tests them at least once per year. The scope of the disaster recovery exercise is to validate the ability to failover a production instance from the primary data center to the secondary data center utilizing developed operational and disaster recovery procedures and documentation. The Covered Services' disaster recovery plans currently have the following target recovery objectives: (a) restoration of the Covered Service (recovery time objective) within 12 hours after Salesforce's declaration of a disaster; and (b) maximum Customer Data loss (recovery point objective) of 4 hours. However, these targets exclude a disaster or multiple disasters causing the compromise of both data centers at the same time, and exclude development and test bed environments, such as the Sandbox service.

More information about Salesforce Disaster Recovery

Change management

Salesforce bases its change management methodology on one main, fundamental principle: trust.
At Salesforce, building trust with customers means pursuing the following three goals.
- Maximizing innovation.
- Minimizing impact.
- Communicating changes.

More information about Salesforce Change Management

Incident management

Salesforce maintains security incident management policies and procedures. Salesforce notifies impacted customers without undue delay of any unauthorized disclosure of their respective Customer Data by Salesforce or its agents of which

Salesforce becomes aware to the extent permitted by law. Salesforce publishes system status information on the Salesforce Trust website. Salesforce typically notifies customers of significant system incidents by email, and for incidents lasting more than one hour, may invite impacted customers to join a conference call about the incident and Salesforce's response.

Data Encryption

The Salesforce Shield Platform Encryption solution encrypts data at rest when stored on our servers, in the database, in search index files, and the file system. To encrypt data at rest and preserve functionality, we built the encryption services natively into the Salesforce Platform.

The Shield Platform Encryption solution uses strong, probabilistic encryption by default on data stored at rest. Shield Platform Encryption uses the Advanced Encryption Standard (AES) with 256-bit keys using CBC mode and a random initialization vector (IV). While this type of encryption results in a loss of some functionality, such as sort operation, we consider this a reasonable tradeoff in favor of security.

More information about Salesforce Data Encryption