



Online **Payslip** Service

ROSCLAR

Security Policy

Employee portal

Table of contents

Contents

Purpose of the document.....	3
Security objective.....	3
Security.....	3
Physical protection of the service	3
Logical protection of the service	4
Security linked to human resources.....	5
Policy on application log-in credentials	5
HTTPS/SSL access	5
Password generation and management.....	6
Random-password creation process test	7
Implemented password policy test.....	8
User account lockout policy test.	9
Storing passwords hashed in database test.....	10
Inactive session policy test	10
Our customer data back-up policy	10
Communications and operations management	11
Business continuity plan	12
Security certificates and added value	12
Legal compliance	12

Purpose of the document

The purpose of this document is to establish the Rosclar Information Security Policy with respect to the service provided by Rosclar involving the a3HRgo application, based on the requirements set out in standard ISO/IEC 27001:2013.

Security objective

The objective is to make sure that all information related to the business processes set out in the scope is handled securely and solely by authorised members of staff. This is how we guarantee the confidentiality, integrity and availability of information belonging to Rosclar customers.

Security

Physical protection of the service

The physical elements required to provide the service, such as the physical servers and main storage systems, are **redundant** and configured for **high availability**, as appropriate, depending on their nature. There are sufficient resources available to ensure that any simple faults in hardware elements will not significantly affect the service while the anomalies are present.

The physical infrastructure for hosting the Rosclar IaaS service is housed in data centres with the necessary specifications to **ensure**:

- the correct temperature of the different hardware elements;
- appropriate environmental humidity;
- an environment free of contaminants such as suspended dust particles;
- uninterrupted power availability, even in the event of failure of the main power supply;
- redundant communications with different operators;
- appropriate protection for events that could damage infrastructures, such as fire;
- the necessary physical security in the buildings, rooms, corridors and panels, with **24x7** access controls.



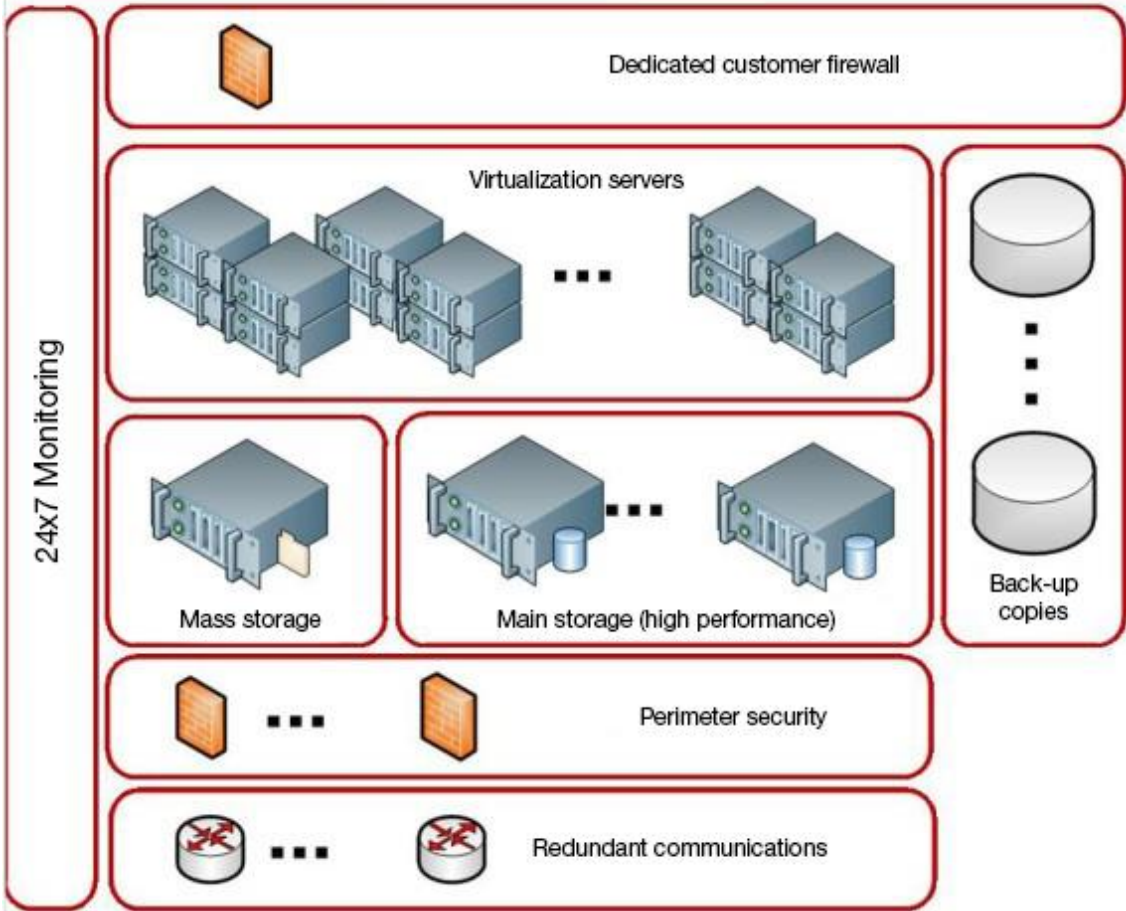
ROSCLAR

Customer services (business applications)





Customer virtual servers and operating systems



Logical protection of the service

Unauthorised access to operating systems is prevented and updating is required to correct any vulnerabilities detected; the appropriate technical security measures will be provided.

Use of unauthorised applications that could invalidate the implemented security measures will be restricted and monitored.

Security linked to human resources

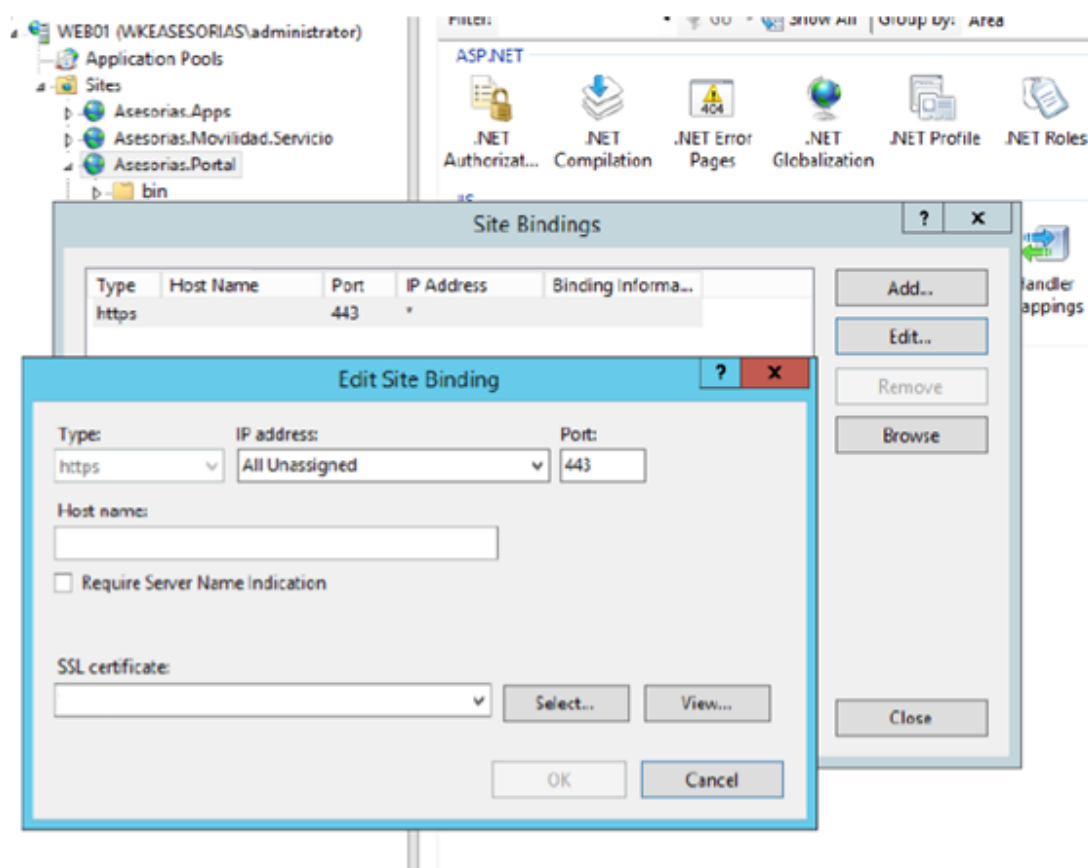
It will be ensured that all employees, contractors and third parties understand their responsibilities and are qualified to perform the duties corresponding to them; this will also reduce the risk of theft, fraud and improper use of the resources made available. It will be ensured that all employees, contractors and third parties are aware of the threats and problems that affect information security and of their responsibilities and obligations, and that they are trained to comply with the organisation's security policy while carrying on their usual work and to reduce the risk of human error. It will be ensured that all employees, contractors and third parties leave the organisation or change workstations in an orderly fashion and without compromising the organisation's security.

Policy on application log-in credentials

Below is a series of tests on all steps that affect the log-in credentials policy to ensure it is secure, that passwords have the required complexity and that everything related to account lockouts and inactive sessions is functioning properly.

HTTPS/SSL access

The image shows the settings for the HTTPS and SSL secure protocols on the servers.



Password generation and management

Automatic password issue generates 10-character passwords in accordance with the following pattern:

- The .NET method `System.Web.Security.Membership.GeneratePassword` is used ([https://msdn.microsoft.com/es-es/library/system.web.security.membership.generatepassword\(v=vs.110\).aspx](https://msdn.microsoft.com/es-es/library/system.web.security.membership.generatepassword(v=vs.110).aspx)), passing 7 and 1 as parameters (7 password characters and at least one non-alphanumeric character).
- The non-alphanumeric character generated by the character “@” is replaced (`Regex.Replace(result, "[^0-9a-zA-Z]+", "@")`).
- “7wX” is added at the end (to ensure there is always a number, lowercase letter and uppercase letter).

Random-password creation process test

The image shows the code that creates random passwords, as described above.

```
public static string GeneratePassword()  
{  
    string result = string.Empty;  
  
    result = System.Web.Security.Membership.GeneratePassword(7, 0);  
    result = Regex.Replace(result, "[^0-9a-zA-Z]+", "@");  
    result += "7wX";  
  
    return result;  
}
```

Here is a sample of the email that is sent:



vi. 01/07/2016 10:20
provision@a3hrgo.com
Bienvenido a A3HRgo!

Para [redacted]

Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.

Acceso a la Solución
Accede directamente a tu cuenta de a3HRgo:
Entrar a Rosclar - Portal del Empleado

Introduzca el siguiente usuario y contraseña (podrá cambiar estos datos una vez esté dentro del programa).

Usuario: [redacted] **Password:** VD@vW@c7wX

Servicios disponibles

Le informamos de los servicios que tiene a su disposición para trabajar con la aplicación y que le ayudarán en el día a día a resolver sus dudas.

Servicio Posventa:

Desde el ícono , situado en la parte superior derecha de la aplicación, podrá realizar consultas o comunicar algún error a nuestro Departamento de Posventa.

Sistema de Ayudas:

Implemented password policy test

The image shows the code that governs the password complexity policy.

```
public static ApplicationUserManager Create()
{
    var manager = new ApplicationUserManager(new UserStore<ApplicationUser>(ApplicationDbContext.Create()));
    // Configure validation logic for usernames
    manager.UserValidator = new UserValidator<ApplicationUser>(manager)
    {
        AllowOnlyAlphanumericUserNames = false,
        RequireUniqueEmail = true
    };
    manager.UserLockoutEnabledByDefault = true;
    manager.DefaultAccountLockoutTimeSpan = new TimeSpan(0, 20, 0);
    manager.MaxFailedAccessAttemptsBeforeLockout = 5;
    // Configure validation logic for passwords
    manager.PasswordValidator = new PasswordValidator
    {
        RequiredLength = 6,
        RequireNonLetterOrDigit = false,
        RequireDigit = true,
        RequireLowercase = true,
        RequireUppercase = true,
    };
    // Register two factor authentication providers. This application uses Phone and Emails as a step of receiving a
    // You can write your own provider and plug in here.
    manager.RegisterTwoFactorProvider("PhoneCode", new PhoneNumberTokenProvider<ApplicationUser>
    {
        MessageFormat = "Your security code is: {0}"
    });
    manager.RegisterTwoFactorProvider("EmailCode", new EmailTokenProvider<ApplicationUser>
    {
        Subject = "Security Code",
        BodyFormat = "Your security code is: {0}"
    });
    manager.EmailService = new EmailService();
    manager.SmsService = new SmsService();

    return manager;
}
```


User account lockout policy test.

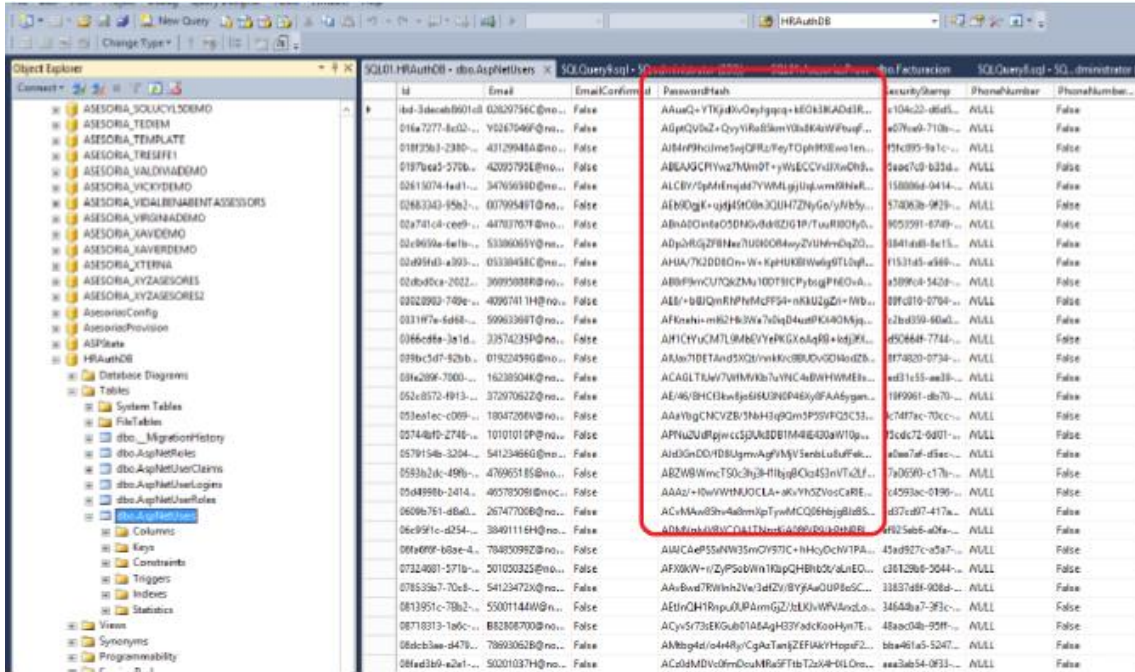
The image shows the code that implements account lockouts and the required inactivity time to execute it. 10

```
public static ApplicationUserManager Create()
{
    var manager = new ApplicationUserManager(new UserStore<ApplicationUser>(ApplicationDbContext.Create
    // Configure validation logic for usernames
    manager.UserValidator = new UserValidator<ApplicationUser>(manager)
    {
        AllowOnlyAlphanumericUserNames = false,
        RequireUniqueEmail = true
    }
    };
    manager.UserLockoutEnabledByDefault = true;
    manager.DefaultAccountLockoutTimeSpan = new TimeSpan(0, 20, 0);
    manager.MaxFailedAccessAttemptsBeforeLockout = 5;
    // Configure validation logic for passwords
    manager.PasswordValidator = new PasswordValidator
    {
        RequiredLength = 6,
        RequireNonLetterOrDigit = false,
        RequireDigit = true,
        RequireLowercase = true,
        RequireUppercase = true,
    };
    // Register two factor authentication providers. This application uses Phone and Emails as a step
    // You can write your own provider and plug in here.
    manager.RegisterTwoFactorProvider("PhoneCode", new PhoneNumberTokenProvider<ApplicationUser>
    {
        MessageFormat = "Your security code is: {0}"
    });
    manager.RegisterTwoFactorProvider("EmailCode", new EmailTokenProvider<ApplicationUser>
    {
        Subject = "Security Code",
        BodyFormat = "Your security code is: {0}"
    });
    manager.EmailService = new EmailService();
    manager.SmsService = new SmsService();

    return manager;
}
```

Storing passwords hashed in database test

The image shows that passwords are not stored in the database in [plaintext](#) but are hashed for greater security.



The screenshot shows a SQL Server Enterprise Manager window displaying a table named 'aspnet_Users' in the 'aspnet' database. The table has columns for 'id', 'Email', 'EmailConfirmed', 'PasswordHash', 'SecurityStamp', 'PhoneNumber', and 'PhoneNumberConfirmed'. The 'PasswordHash' column contains various hashed password strings, such as 'AhuQ+YKj4RvOeyJgq+KQ13KAD4ER...' and 'Ahp2V6aZ+QyyiRa5SmY3a8K4wFbvf...', demonstrating that passwords are stored as hashes rather than in plaintext.

Inactive session policy test

The image shows the code that limits session inactivity time before the session is considered to have expired.

```
// For more information on configuring authentication, please visit http://go.microsoft.com/fwlink/?LinkId=302091
public void ConfigureAuth(IApplicationBuilder app)
{
    // Configure the db context and user manager to use a single instance per request
    app.CreatePerOwinContext<ApplicationDbContext>(ApplicationDbContext.Create);
    app.CreatePerOwinContext<ApplicationUserManager>(ApplicationUserManager.Create);

    // Enable the application to use a cookie to store information for the signed in user
    // and to use a cookie to temporarily store information about a user logging in with a third party login provider
    // Configure the sign in cookie
    app.UseCookieAuthentication(new CookieAuthenticationOptions
    {
        AuthenticationType = DefaultAuthenticationTypes.ApplicationCookie,
        LoginPath = new PathString("/Account/Login"),
        Provider = new CookieAuthenticationProvider
        {
            OnValidateIdentity = SecurityStampValidator.OnValidateIdentity<ApplicationUserManager, ApplicationUser>(
                validateInterval: TimeSpan.FromMinutes(20),
                regenerateIdentity: (manager, user) => user.GenerateUserIdentityAsync(manager)
            ),
            // ExpireTimeSpan = TimeSpan.FromMinutes(20)
        }
    });
}
```

Our customer data back-up policy

As standard, back-up copies are made of the customer's virtual infrastructure (virtual hardware) using the snapshot method. These back-up copies make it possible to quickly recover a machine.

The standard frequency with which back-up copies are made and **how long they are kept**

is explained below:

- a back-up copy is made every night, using the snapshot method;
- back-up copies are kept for 14 days.

Communications and operations management

The security policy regarding communications and operations management is based on the following elements:

- ensuring the correct and secure functioning of information systems;
- implementing and maintaining the appropriate level of information security in the service provision, upholding consistency with any possible third-party service agreements;
- minimising the risk of system failures;
- protecting software and information integrity;
- maintaining the integrity and availability of information and information-processing resources;
- ensuring the protection of network information and support infrastructures;
- avoiding the unauthorised disclosure, alteration, removal or destruction of assets and interruption of customer activities;
- maintaining the security of all information and software exchanged within the organisation and with any third parties;
- identifying any unauthorised information-processing activities.

Business continuity plan

This plan sets out the necessary actions, and the parties responsible for performing them, to enable the organisation to recover from serious incidents such as theft, fire, earthquake, flood, etc., as quickly as possible.

These activities and the parties responsible for performing them are outside the scope of this document, to avoid disclosing confidential information.

Security certificates and added value

We have an ISMS (Information Security Management System) in accordance with the [the good practices set out in standard ISO 27000](#).

We are planning to obtain certification for standard UNE/ISO 27001 this year. We also have members of staff who hold CCIE certification from ISACA.

Legal compliance

Rosclar complies with the current legislation and our processes and data are adapted to the LOPD (Spanish Organic Law 15/1999 of 13 December on Personal Data Protection and Royal Decree 1720/2007 of 21 December, approving the regulations to implement the LOPD).

ROSCLAR