Security Information for HRX

Introduction

Every consideration has been made to ensure the safety of employee data in the HRX system.

In lay terms, we encrypt the data on the server itself so even if, in the unlikely event, someone was able to get access to the server or database or to view transactions, important data is encrypted in the database and in transit when it is requested. This also means that neither HRX nor any of its development team can see your data or tie it back to individuals.

Encryption

Our platform's encryption services provide a simple, convenient interface for encrypting and decrypting text via OpenSSL using AES-256 and AES-128 encryption. All of our platform's encrypted values are signed using a message authentication code (MAC) so that their underlying value cannot be modified or tampered with once encrypted.

Preventing CSRF Requests

Our software automatically generates a CSRF "token" for each active user session managed by the application. This token is used to verify that the authenticated user is the person actually making the requests to the application. Since this token is stored in the user's session and changes each time the session is regenerated, a malicious application is unable to access it.

Protecting Routes

Route filters are used to allow only authenticated users to access a given route and the storage folders are inaccessible from a web browser.

Servers

Our hosting servers are provisioned in the London based AWS data centre. On an account level they utilise IAM security credentials.

This host server has a virtual firewall where by only port 80 and 443 are open to the public (HTTP and HTTPS).

We leverage NGINX as a web server and utilise the provision of SSL certificates.

Our configuration allows for the use of tls1.2 and tls1.3 protocols, only.

What you can do

It is important to keep your log in and your local PC or Mac environment safe and regularly change your password.

PEOPLE

Security Information for HRX

Introduction

Every consideration has been made to ensure the safety of employee data in the HRX system.

In lay terms, we encrypt the data on the server itself so even if, in the unlikely event, someone was able to get access to the server or database or to view transactions, important data is encrypted in the database and in transit when it is requested. This also means that neither HRX nor any of its development team can see your data or tie it back to individuals.

Encryption

Our platform's encryption services provide a simple, convenient interface for encrypting and decrypting text via OpenSSL using AES-256 and AES-128 encryption. All of our platform's encrypted values are signed using a message authentication code (MAC) so that their underlying value cannot be modified or tampered with once encrypted.

Preventing CSRF Requests

Our software automatically generates a CSRF "token" for each active user session managed by the application. This token is used to verify that the authenticated user is the person actually making the requests to the application. Since this token is stored in the user's session and changes each time the session is regenerated, a malicious application is unable to access it.

Protecting Routes

Route filters are used to allow only authenticated users to access a given route and the storage folders are inaccessible from a web browser.

Servers

Our hosting servers are provisioned in the London based AWS data centre. On an account level they utilise IAM security credentials.

This host server has a virtual firewall where by only port 80 and 443 are open to the public (HTTP and HTTPS).

We leverage NGINX as a web server and utilise the provision of SSL certificates.

Our configuration allows for the use of tls1.2 and tls1.3 protocols, only.

What you can do

It is important to keep your log in and your local PC or Mac environment safe and regularly change your password.