EPR FIREWORKS

Security and Data Privacy

EPR systems July 2023

Table of Contents

About Our Company

EPR is a Florida-based company specializing in software specifically for Fire Departments and EMS agencies. We provide a comprehensive records management system as well as data analytics and Training for public safety under one holistic system.

The Product; FireWorks is a complete records management solution for Fire and EMS agencies that enables you to manage all the needs of your department under one systems.

Fireworks is the most modern, innovative system available on the market today. It was developed using best of breed technologies included in Microsoft development architecture, the latest cloud computing service from Amazon, mapping from Google, and turn by turn navigation to the scene by WAZE ™.

The following document describes the steps taken by us to protect your data and comply with the most acceptable information security standards in the industry.
Some of them are as follows:

Infrastructure and Hosting Security

Data privacy and encryption

Backups and disaster recovery

Incident Response

International standards and Compliance

If you have any further questions about
how we protect your data, contact us at

Info@eprsys.com

Infrastructure and Hosting Security

EPR infrastructure and servers managed by Amazon secure data centers (AWS).
There is no 3rd-party access required.
Data / artifacts are not leaving the customer's private environment. Amazon's data center have been accredited under:

ISO 27001
SOC 1 and SOC 2/SSAE 16/ISAE 3402
(Previously SAS 70 Type II)
PCI Level 1
FISMA Moderate
Sarbanes-Oxley (SOX)

Network Security

- Network firewalls built into Amazon VPC, and web application firewall capabilities in AWS WAF let us create private networks, and control access to our instances and applications.
- AWS firewall monitors incoming and outgoing traffic from the servers, allowing or blocking data based
on predetermined security rules.
One of its common uses is to establish a secure separation between a trusted internal network and an external network or the internet.
- We use the Amazon Application Load Balancer (ALB) to protect the system portal from malicious attempts and Denial-of-Service (DoS) attacks. The load balancer distributes incoming application traffic across multiple targets, such as EC2 instances, in multiple Availability Zones. This increases the availability of our application and blocks DoS / DDoS attempts.

Data Security

- Data is encrypted during transit between users' machines. We use industry standard SSL for encrypted communication with SSL protocol version: TLSV1.2

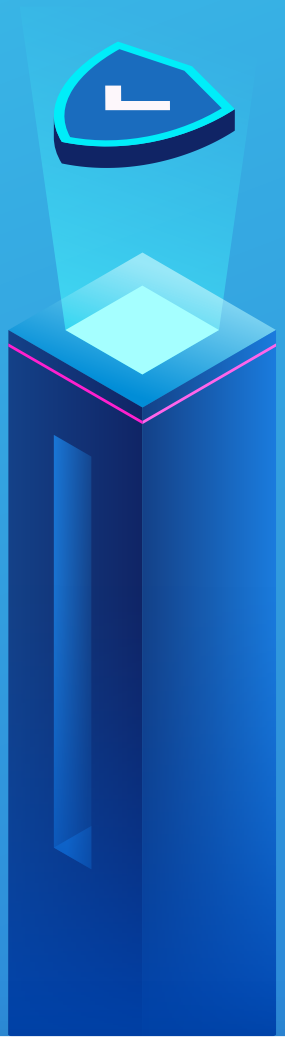
- Information about projects and user data are stored in an isolated SQLserver.

- Sensitive information like passwords and user data is encrypted in our DB.In case of loss, leak, or expiration of your password, it is possible to change it through the Web Portal in a secure way.

- FireWorks using encryption to protect client data and communications, including 256-bit SSL Certification and 2048-bit RSA public keys — the lock icon in the browser indicates that data is fully shielded from access while in transit and data is encrypted over HTTPS when it is transmitted to our central database.

Data privacy and encryption

Data privacy and encryption is a term which stands for a security branch of handling information correctly, storing it securely, handling the data that is shared with third parties and regulations or restrictions of access to the data.



In EPR we store data in a closed and secure environment, we go beyond the international standards of encryption with extra protection steps such as encrypting all the traffic and assuring only those who have access may interact with our services. In addition, the traffic is being monitored and in any case of an incident the response is immediate unauthorized access.

We take data security in the most serious way, compared to the international standards, we encrypt all the traffic within our SaaS cluster with TLS connection.
In addition, we use advanced firewalls\ NLB and apply strict rules and network policies to ensure maximum security and privacy for each user.

The system is being monitored to ensure lack of malicious activity and with the help of a SIEM our response in an emergency case will be immediate and strict to minimize the damage.

Our systems are being regularly backed up and an immediate restore plan is available. The infrastructure is built on AWS and all the privacy policies and precautions for the most secure system are implied in it.

FireWorks Web Portal

Our Web Portal is being monitored for any malicious type of activity, we constantly test it and embrace new ways to protect it.

Prevent attackers from using methods such as SQL injections and brute force attacks. Every connection to the Web Portal UI has a TLS connection to prevent any data exposure in cases of sniffers on a network.

SSL is a technology that keeps the connection between two systems secure and prevents attackers on the network from reading the traffic, it encrypts the traffic between the systems with an algorithm that scrambles the data for those who lack the key won't have the ability to read it.

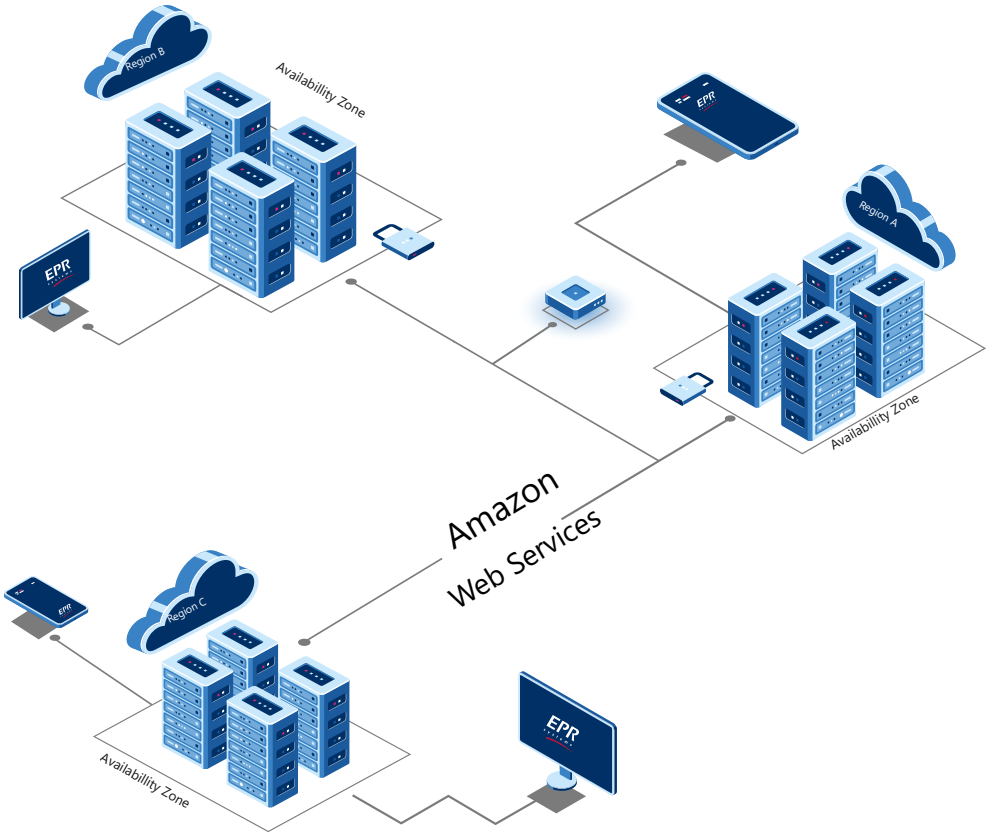
TLS is the successor of SSL, it provides more security and reliability. The encryption process and the connection establishment with TLS enabled servers is more secure than SSL.

Sign up and login credentials are stored in internal and unexposed database. All the stored credentials from the stage are encrypted. On login attempt the password provided by the user is compared to the encrypted one that is stored in the database.

The Portal API internally communicate with the database which isn't exposed to the outer network.
The portal compares the credentials provided by the user with the encrypted credentials in the database.

Backups and Disaster recovery

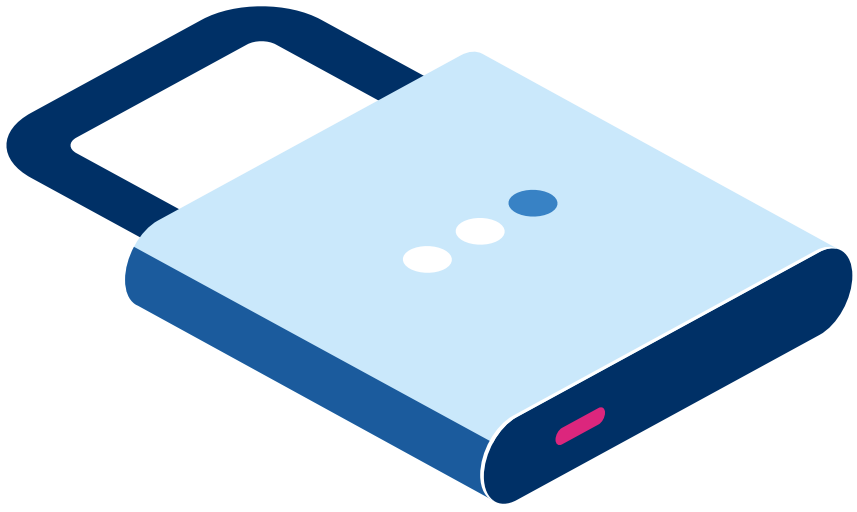
All EPR servers are backed by AWS Region and Availability Zone DRP infrastructure. Each Region is completely independent. Each Availability Zone is isolated, but the Availability Zones in a Region are connected through low-latency links. The following diagram illustrates the relationship between Regions and Availability Zones.



The AWS Global Cloud Infrastructure is the most secure, extensive, and reliable cloud platform.AWS Regions offer low latency, low packet loss, and high overall network quality.
This is achieved with a fully redundant 100 GbE fiber network backbone, often providing many terabits of capacity between Regions.

AWS delivers the highest network availability of any cloud provider. Each region is fully isolated and comprised of multiple AZs, which are fully isolated partitions of the infrastructure. All data flowing across the AWS global network that interconnects datacenters and Regions is automatically encrypted at the physical layer before it leaves the secured facilities

EPR infrastructure is monitored 24/7 to help ensure the confidentiality, integrity, and availability of your data.



DRP

EPR production environment is located on the AWS US East (N.Virginia). Amazon takes a series of steps to ensure low latency, low packet loss, and high overall network quality.

On top of that, we have taken several steps to reduce the dependence on our infrastructure components:

EPR servers are entirely virtual.

All servers work with Elastic Load Balancing (ELB) technology that enables servers to adjust their resources according to a defined plan.

AWS regions are designed to be divided into some availability zones. They separated from each other so that if one area in US East-1 does not respond,
the other is still functioning. This configuration provides us with complete flexibility and availability; if there is an error in one zone, the other can be used as a backup.

User accesses routed through the gateway server, which checks and verifies his identity and provides additional permissions according to the Administrators Settings; only after permissions have been granted they are connected to the selected database.Since the connection is after authentication, the link is transmitted through an automatic monitoring system that routs the Users to the most available server (taking into account several aspects). For example: if the information and Monitoring System Detects that all servers are at maximum capacity, it will add on an additional server (Automatically), and direct the user to the same server.

The DR plan is divided into two levels:

01

First level DR provides a solution to 99.9 percent of fracture cases and is built so that it is activated quickly while Response time is almost immediate.

02

Second level DR for security redundancy, an additional level can be used in a state of very extreme failure.

DR location: for EC2 US East-1, We use three different availability zones; each serves as a DR for the rest. The installation of all systems is divided between the three AZs so that an issue will affect only the part of a system installed in the same AZ.

The AWS EC2 VPC in each of the geographic regions Are divided into a number of isolated locations called Availability Zones. Amazon operates state-of-the-art data centers with high availability.
All available areas in US East (N.Virginia) are self-contained and connected via low latency communication. Availability Zone (AZ) is a data center (one or more) in the AWS area with a redundancy of power, network, and connectivity; working in several availability zones allows us to run the production applications and databases in an optimal configuration can withstand errors without going down.

All availability zones in an AWS area are connected in a high bandwidth connection using low latency Dedicated metro fibers with absolute redundancy, which provide high network output while low retrieval time between Availability zones, All traffic between the availability zones is encrypted.
The network performance can easily withstand performing synchronized duplication between availability zones. If an application is divided between availability zones, the app is more isolated and protected from threats such as Power outages, lightning damage, storms, Earthquakes, and more.

Regular updates to the DR site:

a complete backup of the database to a separate availability zone available every 60 minutes, and at the end of each day Full image.

RPO: Maximum time limit for losing information - is 60 minutes.
RTO: Maximum time to return to full function - 1 hour.

IQNet
THE INTERNATIONAL CERTIFICATION NETWORK

CERTIFICATE

THE STANDARDS INSTITUTION OF ISRAEL AS AN IQNET PARTNER
Hereby certify that the organization

E.P.R. SYSTEMS LTD.
1, Commercial Center, Alei, Israel

For the following scope:

Data security in development and support of systems.

Has implemented and maintains a Information Security Management Service for Health Sector
which fulfils the requirement of the following standard:

ISO27001:2013 And ISO27799:2008

Issued on: 17/12/2018
Date of expiration: 16/12/2021
Date of initial approval: 17/12/2018

Registration number: IL - 103268

Alex Stoichitotu
President of IQNet

Ilan Carmit
Acting Director General

www.sii.org.il

All EPR systems are included in DRP without Exceptions.
There is a written plan and procedures for disaster recovery, which are reviewed in an annual audit (internal and external) every year as part of the ISO 27001 certification.
The audit also requires a routine of exercises conducted on a regular basis in relevant outlines; both planned or by surprise.

Separate domestic geographical area - extreme cases

Domestic data preservation

Understanding the importance of maintaining all data domestically, both the primary AZ, located in Virginia as well as the redundancy mirror site in California, are US based.

Availability zones are significantly physically separated, although they are no More than 100 km from each other. In order to prepare for the most extreme cases of destruction in the vicinity of AWS US East-1, we opened a Separate environment in another domestic geographical area – AWS California. This secondary environment it utilized as a security line to ensure data protection.

AWS sites in US East (N.Virginia) and US West (California) meet the strictest standards for data center management and are managed with the best management tools. In addition, we use monitoring and control tools, including DLP monitoring and control systems, to ensure the ongoing functioning of the servers and the prevention of errors in advance. A risk assessment is conducted once a year and is valid for one year.

Data Backup Procedures

Our backup strategy consists of backup procedures on an hourly, daily, weekly, monthly up to 24-month basis.
To reduce the risk of data loss, we move the backup snapshots every night to a Separate AWS environment in California.

EPR technical staff tests the integrity of the backups on a weekly basis.

Incident Response

The EPR Incident Response Plan has been developed to provide direction and focus to the handling of information security incidents that adversely affect EPR Information Resources. The EPR Incident Response Plan applies to any person or entity charged by the EPR Incident Response Commander with a response to information security related incidents at the company, and specifically those incidents that affect EPR Information Resources. The purpose of the Incident Response Plan is to allow EPR to respond quickly and appropriately to:

Event Definition

Any observable occurrence in a system, network, environment, process, workflow, or personnel. Events may or may not be negative in nature.

Adverse Events Definition

Events with a negative consequence. This plan only applies to adverse events that are computer security related, not those caused by natural disasters, power failures, etc.

Incident Definition

A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices that jeopardizes the confidentiality, integrity, or availability of information resources or operations.

A security incident may have one or more of the following characteristics:

A. Violation of an explicit or implied EPR security policy
B. Attempts to gain unauthorized access to a EPR Information Resource
C. Denial of service to a EPR Information Resource
D. Unauthorized use of EPR Information Resources
E. Unauthorized modification of EPR information
F. Loss of EPR Confidential or Protected information

International standards and Compliance

In recent years, there is a growing consciousness of the need to secure the authority's information and protect it from malicious elements trying to hack in and make use of your data. Many changes have taken place in favor of the responsibility for, and protection of your information with the amendment of the Privacy Protection Act in May 2018. EPR was prepared for these changes in advance, as the company provides services under the most stringent conditions to hospitals and other medical organizations across the United States.

We are certified and comply with international standards that indicate the highest level of information security:

ISO 9001

Quality Management at EPR Systems, especially in the service field.

ISO 27001

Establishment, management, and maintenance of the data security at EPR Systems.

ISO 27799

Management and data security in the healthcare systems of EPR infrastructure.

HIPAA Statement

Management and protection of medical information and of all related actions on the EPR infrastructure.

Compliance with the Privacy Protection Act and its amendment, including:

1. Guidance on compliance with the Privacy Protection Act.
2. Meeting the highest levels of security for all the organization's servers.
3. Conducting a risk survey, and penetration tests performed by a leading security company.

Vulnerability Remediation

The vulnerability remediation process is a workflow that fixes or neutralizes detected weaknesses. It includes 4 steps: finding vulnerabilities through scanning and testing, prioritizing, fixing, and monitoring vulnerabilities.

Our complete process:

01

Find: Detecting vulnerabilities through routine scanning and testing.

02

Prioritize: Understanding which vulnerabilities pose a real and significant risk.

03

Fix: Patching, blocking, or otherwise fixing vulnerabilities at scale and in real-time.

04

Monitor: Automatically monitor projects and code for newly discovered vulnerabilities, with real-time alerts and notifications via all the relevant channels.

You are in safe hands with EPR Systems