

## Our Promise to Clients

# Security Features

The SOC II-certified safety checks, tools, and policies keeping your data secure.


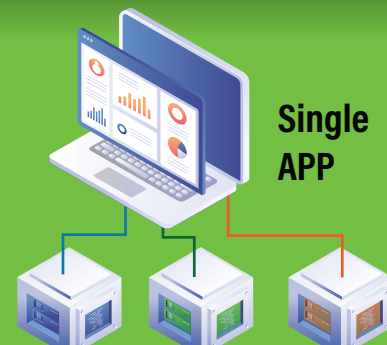

ERA is committed to providing the most reliable and comprehensive software in the EHS market. Our platform has a 99.6% uptime, and its cloud-hosted nature means clients do not have to pay for additional equipment, servers, or software licenses—we cover the cost of guaranteeing your data remains intact.

Security is built into our company culture, from the extensive Certn background check we run on our new employees to the two-factor authentication protocols they follow every day. Our efforts to protect sensitive data have earned us a **SOC II, Type 2 certificate** from Audit Peak; Drata, a third-party platform, regularly monitors our software environments and local machines for proof of compliance with these SOC II standards.

## ERA's Centralized Multi-Tenant System

Every client gets their own dedicated database within our application, preventing unauthorized access while expediting the debugging process and keeping development costs low (relative to single-tenant systems).

**BEST CHOICE** **ERA'S OFFER**

Shared Application	✗	✓	✓
Separate Database	✓	✓	✗
Tenant type	Single Tenant	Multi-Tenant - Option 1	Multi-Tenant - Option 2
Multi-Clients	Multi-APP A,B,C 	Single APP 	Single APP 
	Multi-database A,B,C	Multi-database A,B,C	Single-database

# Data Retention – An Overview

Client data is stored within our platform from the moment it is loaded into the system to the day the client stops being an active customer. At the conclusion of the contractual agreement, we detach and delete the client's database, thus purging all data from the production environment. Unless otherwise requested by the client, a last backup is taken and kept for a period of 365 days, as stipulated by SOC II requirements.

## A Complete Toolset

By working alongside a variety of commercial-licensed software (never freeware), ERA is able to put in place several bank-level security measures that make unauthorized access to your data, or its deletion, practically impossible.



### Regular backups

Nightly differential and weekly full backups with Acronis.



### Airtight data centers

24/7 CCTV footage, uninterruptible power supply, and protection against fires, climate, and temperature variabilities.



### Controlled entry to production environment

Remote access to production systems restricted to authorized employees with a valid Entra ID MFA token over an encrypted VPN connection.



### Anti-malware technology

Sentinel One anti-virus deployed on all environments and endpoints commonly susceptible to malicious attacks.



### Annual penetration testing

Evidence-based pen tests conducted by BreachLock for the identification (and prompt remediation) of vulnerabilities across our internal and external attack surface.



### Data redundancies

Minimal disruption to the availability of customer data with redundancies in four distinct data centers, powered by Azure.



### A first-class infrastructure

Azure-hosted firewall, databases encrypted at rest, and security information and event management (SIEM) solution.



### Vulnerability scanning

Identification and remediation of potential security flaws in ERA source code through Veracode static and dynamic analysis.



### Two-factor authentication

Another layer of security for your users' login process with 2FA via one-time passwords (OTP) sent by email.



### Single sign-on

Cross-domain SSO compatible with any system utilizing the SAML 2.0 standard for streamlined access.



## Any other questions about security?

We'd be happy to discuss your unique security requirements. You can reach us at the email address and phone number listed below.