Ecaresoft: Security Processes 2023

Version 2.4.1

July 2024

Notice

The information contained in this document is presented for informational purposes, and presents the security processes that support the current offer of Ecaresoft services, which may be subject to change without prior notice, and does not represent a commitment for Ecaresoft.

Abstract

This document describes the operational security processes for the infrastructure and applications developed by Ecaresoft.

Table of Contents

nimbo

E-CS

Introduction

Ecaresoft develops software for the health industry. **Cirrus**, an EHR, HIS and ERP that facilitates the hospital care centers administration; **Nimbo**, a comprehensive solution for small outpatient clinics and medical teleconsultation; **Estela**, a business intelligence (BI) system that helps decision makers in hospital care centers. The confidentiality protection, the integrity and availability of our clients' information is the most important thing to Ecaresoft.

Ecaresoft compliance program

Ecaresoft complies with the security and privacy criteria established by some organizations, such as the certification program of the Government of the United States of America, issued by the Office National Coordinator (ONC) of Health Information Technology (HIT), in the domains:

- 170.315 (d)(1) Authentication, access control, authorization
- 170.315 (d)(2) Auditable events and tamper resistance
- 170.315 (d)(5) Automatic log-off
- 170.315 (d)(6) Emergency access
- 170.315 (d)(8) Integrity
- 170.315 (d)(10) Auditing actions on health information
- 170.315 (d)(12) Encrypt authentication credentials

Additionally, the infrastructure that is being used to run Ecaresoft's applications complies with some specific standards, including:

- Cloud Security Alliance (CSA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI-DSS) level 1
- ISO 27001
- Federal Information Security Act (FISMA) Moderate
- Federal Risk and Authorization Management Program (FedRAMP)
- SOC1 and SOC2

Business Continuity Management

Ecaresoft's infrastructure is based on the cloud, specifically on **Amazon Web Services (AWS), and Heroku Platform,** which allows for a high level of availability and a resilient IT architecture. The security model followed is the **shared responsibility model** in cloud-based services for **Software as a Service (SaaS)**.

Availability

Ecaresoft services are distributed in clusters in two global regions: **US West (Oregon) and Middle East (Bahrain) for AWS, and in US East (Virginia) for Heroku**, with self-healing capacity in case of hardware failure where critical services are executed. This self-healing capability allows services to be automatically deployed in a new instance in case of a physical failure, with this approach services are available and operating in a few minutes.

In both AWS regions, **US West (Oregon) and Middle East (Bahrain)**, there is an additional alternate site for an online database replication in a different Availability Zone **(AZ)** in **dual active** mode, and the data lake for **business intelligence.**

Incident Response

The Cloud platform incident response teams use industry standard procedures to solve events that may affect the continuity of Ecaresoft's productive services with a **24x7x365** coverage to detect incidents and manage their impact and resolution. Ecaresoft's operations team handles application and platform incidents with the same coverage and additional ones depending on the clients need.

Disaster Recovery

The infrastructure in the Cloud is in the process of migrating from Platform as a Service to **Infrastructure as Code**, which will allow us to restore our services with an **RTO** of a few hours in case of eventualities.

Communication

Ecaresoft has implemented different internal communication methods globally to help its employees to understand their individual responsibilities and communicate relevant events, such as orientation and training programs for new hires, regular management meetings to publish business performance and other related topics, and electronic media such as videoconferences, instant messaging and email, in addition to the publication in the internal communications channel.

Network Security

The Ecaresoft network in the AWS cloud (**Virtual Private Cloud (VPC)**) has been designed to have the level of security required by the type of information that is handled in the different application components and the demand of the flow of information, following the best practices recommended by the AWS cloud provider.

Ecaresoft's network infrastructure in the AWS Cloud is being continuously managed and monitored. Each server and device automatically reports its health status reporting some indicators such as **processor usage, memory, bandwidth, disk space** among some other technical metrics. In the event that a metric exceeds a defined threshold, an automatic alert is sent to the operators to warn of a potential problem and to be able to proactively take the appropriate actions.

Network security architecture

At Ecaresoft's AWS cloud, network devices are implemented, including **firewalls** and other border security devices, to monitor and control communications between the productive network and the Internet, in a private network model **(Single Tenant Network).** These devices use a specific set of rules, access control lists, security groups for specific ports and settings to restrict the flow of information to / from Ecaresoft application services.

Access control lists and traffic security groups are configured on device interfaces and they complement the ones defined by AWS, which are always automatically updated.

Transmission protection

All connections to the Ecaresoft services and applications are made, depending on their criticality, by **HTTP** or **HTTPS** using **Transport Layer Security (TLS)**, a cryptographic protocol designed to protect against **eavesdropping**, manipulation **(tampering)** and falsification **(forgery)** of messages. File transmissions are made by **SFTP (Secure File Transfer Protocol)**. TLS certificates for secure communications use the **RSA** encryption algorithm with **2048**-bit keys and **SHA-256** with RSA for digital signature.

For certain specific cases that may require connections to external on-premises services, an IPsec **Virtual Private Network (VPN)** has been established to provide an encrypted tunnel between the client's physical facilities and the AWS **Virtual Private Cloud (VPC)** where the ecaresoft services are hosted.

Corporate Segregation

Logically, Ecaresoft's productive network **(Virtual Private Cloud (VPC)** in AWS) is independent and separated from the corporate network **on-premises.** Access to the productive network in AWS is limited to system administration personnel, and in the event that access is required by someone else, it is explicitly requested and authorized, and it is revoked once the tasks for which the access was requested are completed. All accesses are granted aways under the principle of least privilege. Access through remote terminals for administration is done through security certificates in **PEM** files, and not by password.

Fault Tolerant Design

Ecaresoft's productive infrastructure, which is being built on the AWS cloud, allows it to have a **minimal impact in case of system or hardware failures (fault tolerant design)**. Additionally, the design of the logical architecture of the services is constantly improved to offer high availability in the critical components and services.

Access to the application services is done through a **load balancer** that distributes user sessions among the different active application servers, based on the current load of each server and the source IP address of the traffic, among other factors and, in case of unavailability of any server, the traffic of the user sessions is redirected to another active server. The architecture is **resilient** since the application servers are located in at least **2 availability zones (AZ)** so that if one of them is affected by the AWS cloud provider (unavailable because of a network or hardware failure), the service remains online and working since there is another server in another Availability Zone.

Change Management

Scheduled and emergency changes to existing infrastructure configurations go through a process of testing, authorization and documentation, seeking to minimize any impact to customers and end users. Ecaresoft communicates to the customers via email or through the health monitoring site when a service is being or is about to be affected, mainly in planned events due to major / minor updates to the Ecaresoft’s products or even due to some unplanned event or infrastructure adjustment.

Accesses in Ecaresoft

Ecaresoft's productive network is independent from the corporate network and applications, so access control is also independent.

Accounts' review and audit

The user accounts are reviewed periodically to verify that they have the level of permissions according to the role that was assigned to each user. Employee accesses are revoked as soon as they leave Ecaresoft company. User accounts that were provided to use Ecaresoft's applications and services are deactivated as well.

User accounts are managed by each client organization, who is responsible for registering, assigning privileges and deactivating them when they are no longer required.

Accountability

Through our AWS and Heroku Cloud providers, we keep **logs** of access to our services, which are **audited** and analyzed frequently, and kept for up to one year. An important functionality related to the logs is that we have an infrastructure to **audit** the activities of the end users if required, maintaining confidentiality in the logs at all times, since no sensitive data is recorded, however with **audit logs** it is possible to **track** the actions taken in case of failures or even of any **compliance** investigation, with the aim of **non-repudiation** and **accountability**.

Application Security at Ecaresoft

Ecaresoft provides a variety of account security controls to prevent unauthorized access to applications and **APIs (Application Programming Interface).** This includes credentials for access control, **HTTPS encrypted data transmission**, and **user activity logs**.

To ensure that only authorized users and processes can access Ecaresoft application resources, different types of credentials are used for authentication. These include **passwords**, **cryptographic keys**, **digital signatures**, and **certificates**.

Each user has access to their data through individual accounts or credentials with access control **(authentication, authorization, session management** and **activity log)** managed by each organization. Ecaresoft staff cannot access the applications through user credentials, so access to the data of each organization is done exclusively through their associated accounts.

For security, if the credentials are forgotten, it is only possible to recover them through an automated password regeneration process. It is not possible to receive them by any other means such as email, because they are stored as irreversible **one-way hashes**.

The consolidated data reports which belong to each organization are not stored persistently on Ecaresoft's servers, however they are generated on demand, with controlled access and expiration date to view them.

Self Design Principles

Ecaresoft's development process follows secure software development life cycle **(SDL)** best practices, which include formal design reviews, threat modeling, and risk analysis, as well as secure development practices against application vulnerabilities and malicious code injections such as **Cross-Site Scripting (XSS), SQL injection (SQLi), buffer overflows**, among others, based on **OWASP** recommended practices.

The static analysis of code using Security Automated Tools **(SAST)** is part of the standard software build process, and productive software undergoes periodic regression, penetration testing, and **DAST** when major product releases are made. Also, during the continuous integration (CI) process, all libraries used by Nimbo and other API are automatically analyzed and reviewed against public vulnerability databases, such as **CVE**.

Application security reviews begin during the design phase and are maintained until they are released to end-user operation.

Database Security

The Ecaresoft application databases are implemented on **RDS (Relational Database Service)** in the AWS cloud, which allows automated **backups and failovers.** Access to the databases is configured to only allow connections from the application network **(VPC),** so even administrative access from the outside is restricted. The disks where the database information is stored are **encrypted** with the help of the **AWS Key Management Service (KMS)**, which is an additional security point to restricted access. Only the database administrator can access it if strictly necessary.

The **demographic data of the patients** is stored in the database **encrypted** with a symmetric algorithm **AES (Advanced Encryption Standard)** with a private key of 256 bits. So they can only be visible through the corresponding application.

Database backups are gotten automatically through **DB snapshots,** allowing any instance to be restored in a matter of minutes. DB Backups history are configured from **3 days for non-productive databases** to **one week for productive databases**. Additionally, an always up-to-date synchronous replica of the database is maintained in a different geographical availability zone (In the same region but in a different Availability Zone **(AZ)**. As an additional alternative, incremental backups are made every 3rd. using the corresponding utility of the **PostgreSQL V14.2** database engine **(pg_dump)**, they are stored in the **Simple Storage Service (S3)** with specific retention rules that were defined by Ecaresoft.

For the Nimbo production database daily backups are stored for the last week, weekly backups are stored for the last 4 weeks and monthly backups are stored for the las 12 months. These backups are safely stored in an S3 with replication and encryption at rest using AES-256.

The information belonging to a client can be requested throughout the official communications channels, once the request is validated and processed the information will be shared in CSV files, those files are compatible with most offimatic software. The time required to process the request depends on the data size and availability of resources. Most requests are resolved around 5 bussines days.

Application Access Control

Authentication is achieved through federation with Google Authenticator using the IETF **OAuth** standard, with the ability to integrate other **federated authentication** entities as required.

User management and role management are part of the account lifecycle, which is managed granularly by each organization through an administration interface, so access control and role granting is discretionary, and it can be audited at any time for non-repudiation.

Documentary Review

Date	Description
2017	Document creation
2020	Minor updates
June 2021	Migration to a new format
August 2021	Technical details added
July 2022	Technical review and creation of english version
August 2022	Minor updates
November 2023	Adding backup retention policy and data handout policy in Nimbo