factoro

Liquidez garantizada

Security Documentation

PROPRIETARY INFORMATION

This document is the property of Factoro; it contains information that is proprietary, confidential, or otherwise restricted from disclosure. Dissemination, distribution, copying or use of this document in whole or in part by anyone other than Factoro is strictly prohibited.

Table of Contents

Introduction

Factoro delivers a scalable application with high availability and dependability. Protecting the confidentiality, integrity and availability of our customer's data is of paramount importance to Factoro, as is maintaining customer trust and confidence. This document is intended to summarize Factoro's standards compliance, security framework and operational practices.

Factoro Compliance

SOC 2

Factoro has implemented effective controls for all required SOC 2 criteria. An independent audit is conducted annually to ensure continued compliance. The most recent SOC 2 report is available upon request.

SOC 3

The SOC 3 report summarizes our organization's controls relevant to security, availability, processing integrity, confidentiality and privacy, and is written by an independent auditor.

Penetration Testing

Internal and external penetration tests are conducted annually by an independent security organization. Any vulnerabilities found are documented and immediately remediated. Post mortem analysis is performed to identify root cause and implement future controls.

Factoro Customer Data

Encryption

All of our customer data is encrypted both in transit and at rest using one or more of the following algorithms/protocols:

- SHA-256
- AES-265
- 3DES
- Blowfish
- TLS / SSL
- PGP
- GKMS / KMS

Content

Factoro is required to store certain files locally according to Mexican law.
The following files can be summarized as:

1. Award
2. Control
3. Division
4. Invoice
5. Organization
6. User

Transmission

Factoro uses a variety of secure options for the transmission of customer data, all of which are encrypted in transit:

- FTPeS
- SFTP

Storage

All customer data is separated and stored in an encrypted AWS S3 bucket. Factoro uses security methods which prevent customers from accessing anything but their own data. Data required to be stored in Mexico is stored accordingly.

Amazon Web Services (AWS) Compliance and Infrastructure

Factoro uses AWS for hosting systems and services, following best practices and implementations. In this section we cover both the security and high availability features we are leveraging.

Compliance

Factoro reviews AWS's compliance reports monthly.
To date, AWS is compliant with the following standards:

- SSAE16 / ISAE3402
  - SOC 1
  - SOC 2
  - SOC 3
- FISMA
- DIACAP
- FedRAMP
- DOD CSM Levels 1-5
- PCIDSS Level 1
- EU Model Clauses
- ISO 9001 / ISO 27001 / ISO 27017 / ISO 27018
- ITAR
- FIPS 140-2
- MLPS Level 3
- MTCS
- CJIS
- CSA
- FERPA
- HIPAA

- MPAA

Physical Security

AWS data centers are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff. AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to data centers by AWS employees is logged and audited routinely.

Redundancy

AWS data centers are designed to anticipate and tolerate failure while maintaining service levels. Data centers are built in clusters in various global regions. All data centers are online and serving traffic; no data center is “cold.” In case of failure, automated processes move traffic away from the affected area. Core applications are deployed to an N+1 standard, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

Fire Detection and Suppression

Automatic fire detection and suppression equipment are installed to reduce risk. The fire detection system utilizes smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems.

Power

AWS data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Generators are used to provide back-up power for the entire facility.

Climate and Temperature

Climate control is required to maintain a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages. AWS data centers are conditioned to maintain atmospheric conditions at specified levels. Personnel and systems monitor and control temperature and humidity at appropriate levels.

Storage Device Decommissioning

When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices.

System Monitoring

AWS monitors all support systems and equipment so that any issues are immediately identified. Preventative maintenance is performed to maintain the continued operability of equipment.

Factoro High Availability Strategy

The objective of this section is to emphasize some of the steps Factoro has taken in order to deliver high system availability for all users. All of our systems are designed and engineered with the purpose of minimizing and/or eliminating critical points of failure. In essence, if one component in our system fails it will not disable the entire system for any significant amount of time.

Redundancy Facilities

All of our systems and data are replicated in secure facilities in separate geographic locations. In the event of an interruption our systems will automatically detect the failure and take appropriate measures to restore system availability.

Telephone Infrastructure

All of our systems are VOIP-based and provided by Axtel which enables routing of incoming calls to any end point destination, ensuring your call will be attended.

Internet and LAN Security

Enterprise level Internet services are provided at Factoro's headquarters, with redundant ISPs and dedicated fiber optic circuits. All services are monitored and protected by industry leading application delivery controllers.

Internet security is provided by redundant firewalls and an IDS.

Database Management

Factoro deploys scalable database systems across multiple availability zones and regions. Each zone is geographically separated to avoid a single point of failure, and data replicates to all zones in real time.

Mass Storage Systems

Factoro uses mass storage data systems built in clusters, capable of dynamic or on-demand expansion. These clusters are distributed among various global regions and are designed to tolerate hardware failures while maintaining required service levels.

Backups

Factoro uses a number of IAAS provided tools for backup management. All backups are encrypted in transit and at rest. Redundant backup copies are stored across multiple availability zones and/or regions. Backup frequency and retention vary depending on the critical nature of the data and/or system.

Hardware and Infrastructure

Configuration management software is installed when new hardware is provisioned. Updates by IAAS providers are done in such a manner that, in the vast majority of cases, will not impact the customer and their service. When service may be adversely affected, IAAS providers communicate the change(s) prior to implementing.

Capacity Management

Factoro uses AWS Elastic Compute Cloud (EC2), which provides resizable computing capacity using servers' instances in state-of-the-art data centers. EC2 makes web-scale computing easier by enabling dynamic scaling with minimal friction.

Maintenance and Failure Allowance

Factoro's redundant architecture allows shutting down parts of systems for maintenance or replacement with little or no impact on our required capacity at a given time.

Our system allows for rapid expansion of system capacity should the need arise. Internet services are burstable, meaning unexpected spikes in bandwidth utilization are handled with no intervention.

Factoro Security Policy & Procedure Framework

The objective of this section is to emphasize Factoro's security framework. Only keep policies and procedures are covered in this section. Please contact an associate to review additional policies.

Background Checks

Factoro screens all associates prior to employment, which includes a background investigation. Issues identified during background checks are resolved prior to employment and prior to provisioning access to Factoro systems.

Security Awareness Training

All Factoro associates are required to complete an online information security awareness training course within the first 30 days of employment. Additional training is provided, and all security policies reviewed, in the new associate IT orientation which also occurs during the first month of employment. All activities and results are documented and retained indefinitely.

Information Security

This policy defines what we consider to be confidential and third-party confidential information, how that information can be shared both internally and externally, how and where that information can be stored, and how it is labeled. These definitions inform most other security policies as they're the basis for which we determine secure solutions and audit compliance.

Secure Desk & Screen

Factoro associates are prohibited from keeping any confidential or third-party confidential information in view at their work area. This sensitive data is required to be kept in a locked compartment or at a minimum concealed from view. When unattended, all workstations are required to be locked and password protected.

Access Control

Risk Management

Factoro conducts an internal risk assessment annually to identify and remediate any known vulnerabilities. The entire assessment process is documented and audited annually by an independent party as part of the SOC 2 process.

Password Requirements, Account Lockouts & MFA

Passwords are expired frequently - exact frequency varies depending on the sensitivity of the system. Complexity requirements are enforced and follow industry best practices. Accounts automatically lock after 3 failed login attempts. 2FA is enforced wherever necessary.

Mobile Device Management

Factoro maintains the ability to remotely wipe all data from any associate's mobile phone or tablet containing Factoro data. Devices are screened and only allowed connectivity to Factoro services after meeting security policy standards.

System & Event Logging

Access and system event logs are captured on all resources and stored in a number of repositories. Reviewing and reporting responsibilities are clearly defined, as are schedules and escalation. All logs are retained indefinitely.

Intrusion Detection System (IDS)

Factoro leverages intrusion detection to perform real-time scans and identify threats and trends. An intrusion detection alerts an on-call resource, who responds and escalates in accordance with internal requirements. Threats, responses, remediation, and post mortem are documented thoroughly and retained indefinitely.