CaféX Communications Information Security Whitepaper

Contents

Glossary of Terms

Word	Meaning
PCI-DSS	Payment Card Industry Data Security Standard
ISO27001	International Standard for Information Security Management Systems
HIPAA	Health Insurance Portability and Accountability Act
BAA	Business Associate Agreement
GDPR	General Data Protection Regulations
CIS-20	Center for Internet Security
OWASP	Open Web Application Security Project
NIST	National Institute of Standards and Technology
SOC	Service Organization Control

Introduction

CaféX creates software that makes it simple for people to collaborate in ways that work best for them - from software development to enterprise sales to everyday customer support. Whatever the use case for our services, security is our top priority.

Our customers trust us with their data and that is not something we take lightly. We combine enterprise-class security features with comprehensive audits of our applications, systems, and networks to ensure customer and business data is always protected.

Security Model

Our security model prioritizes three key provisions:

1. A secure and compliant business environment for our customers
2. Always-up service and agile response to incidents
3. User-friendliness for our customers and customers' customers

Technical security is key, however, security goes beyond that: it is an organisational effort. CaféX runs a comprehensive security and compliance programme by continuously looking for risks that could lead to breaches, downtime and non-compliances. Our efforts cover:

- Internal policies and a comprehensive cyber security programme
- Certifications or external assessments such as PCI/DSS, ISO 27001, HIPAA (via BAA), Privacy Shield and EU-GDPR
- A set of technical procedures to run our infrastructure, inspired by proven frameworks such as CIS-20, OWASP or NIST
- A Secure Software Development model
- Security-minded operations able to provide fast support and response to an incident
- Well-defined requirements for our Partners, Suppliers and Contractors

Security Organization & Program

While security is a high priority for all teams, a dedicated Security Team manages CaféX's security program. The CaféX security framework is based on the ISO 27001 Information Security Standard and includes programs covering: Policies and Procedures, Asset Management, Access Management, Cryptography, Physical Security, Operations Security, Communications Security, Business Continuity Security, People Security, Product Security, Cloud and Network Infrastructure Security, Security Compliance, Third-Party Security, Vulnerability Management, as well as Security Monitoring and Incident Response.

Security is represented at the highest levels of the company. Our Chief Information Security Officer meets with executive management regularly to discuss issues and coordinate company-wide security initiatives. Information security policies and standards are approved by management and available to all CaféX employees, partners, suppliers and contractors.

People Security

People are our best assets. We've implemented processes to ensure we're bringing in qualified people and keeping them up to date on the latest security trends. Here are some of the processes we have in place:

Background Checks

All candidates in the USA must pass stringent background checks by a specialized third party before being offered a position. For domestic candidates, these checks include: Social Security Number trace, criminal county search (7-Year address history), multi-state instant criminal, National Sex Offenders Public Registry, Office of Foreign Assets, professional references, and education verification.

For international new hires, the background check includes (where allowable by law): international criminal search and education verification.

Information Security Training

All new employees attend Security Awareness Training which is given upon hire. Our Information Security Awareness Program runs continually over the entire year for all employees, providing policies, advice and guidance as well as keeping all our employees up to date with the latest security news and threats.

Contractors & Third Parties

In the event that CaféX retains the services of any outside service partners, CaféX will insist that those companies perform similar background checks on their own employees. If the contractor is an individual, he or she must submit to a background check administered by CaféX before being allowed to work for us.

Product Security

Our products and services are secured by design, from both operations and development perspectives. To protect data-in-motion, data-in-use, and data-at-rest, we ensure the use of industry standard secure protocols and best practices.

Secure by Design

CaféX security engineers continuously perform activities to ensure that our products are secure, including:

- Internal security reviews before products are launched
- Regular penetration tests performed by third-party contractors
- Continuously running internal and external security tests

Penetration Testing

We employ third-party, Crest-Approved security experts to perform detailed penetration tests on different applications within our family of products. Our Penetration Testing is done every 6 months and at the time of every major release.

Physical Security

Physical security is an important part of CaféX's security strategy. We're committed to securing our facilities.

Datacenter Security

CaféX leverages Microsoft Azure centers for all production systems and customer data. Azure follows industry best practices and complies with an impressive array of standards.

For more information on Microsoft Azure Data Center Physical Security, see Microsoft's Azure Security Whitepaper: https://cafex.to/azuresecurity

Office Location Security

CaféX has a security program that manages visitors, building entrances, CCTVs, and overall office security. All contractors and visitors are required to wear identification badges.

Third Party Suppliers

When market opportunities suggest that CaféX should partner with other technology companies, we will require that they follow the same rigorous standards as our own. Namely, they must be ISO 27001 and SOC 2 certified, perform the same screening of their employees, and their software solutions be equally as secure.

Cloud & Network Infrastructure Security

The security of our infrastructure and networks is critical. Knowing our service remains confidential, available and its integrity remains in tact is key to what we do.

Infrastructure Management

Direct access to production resources is restricted to employees requiring access and requires approval, strong multifactor authentication, and access via a bastion host.

Data Segregation

The CaféX cloud production environments are designed to be multi-tenant and therefore, although sharing the same underlying highly available resources, care is taken to ensure all customer data is logically isolated. Production and non-production networks are segregated. All network access between production hosts is restricted using firewalls to allow only authorized services to interact with the production network.

24/7 Monitoring

All Production Network systems, networked devices, and circuits are constantly monitored and logically administered by CaféX staff.

Business Continuity and Disaster Recovery

CaféX uses a variety of tools and mechanisms to ensure best-in-class resiliency.

Recovery Planning

CaféX maintains formal Business Continuity and Disaster Recovery plans that are regularly tested, reviewed and updated.

Global Resilience

Hosting our services using high-availability architecture within Microsoft Azure and Amazon Web Services gives CaféX the ability to remain resilient globally - even if one location goes down. Both Microsoft Azure and Amazon Web Services span multiple geographic regions and availability zones, which allow our services to remain resilient in the event of most failure modes, including natural disasters or system failures.

Security Compliance

CaféX is committed to mitigating risk and ensuring that CaféX services meet regulatory and security compliance requirements.

Regulatory Environment

CaféX complies with applicable legal, industry, and regulatory requirements as well as industry best practices.

Top Tier Infrastructure Provider

CaféX cloud communications platform is hosted at Microsoft Azure data centers, which are highly scalable, secure, and reliable. Azure complies with leading security policies and frameworks, including SSAE 16, SOC framework, ISO 27001 and PCI DSS.

ISO 27001

ISO 27001 is a globally recognised certification, which means, wherever our customers are located, they can be assured that CaféX adheres to a consistent set of standards approved worldwide.

Our ISO27001:2013 certificate of compliance is available here

SSAE 16 SOC2 Type 2

The successful completion of our SOC 2 ® Type I examination audit provides our clients with the assurance that the controls and safeguards we employ to protect and secure their data are in line industry standards and best practices

Our Certificate is available here

Our Type 1 report is available subject to NDA, please contact your account manager or email compliance@cafex.com

We are working towards our Type 2 certification and will be available in May 2019

GDPR

CaféX Communications ('we' or 'us' or 'our') are committed to ensuring the security and protection of the personal information that we process, and to provide a compliant and consistent approach to data protection. We have always had a robust and effective data protection program in place which complies with existing law and abides by the data protection principles. However, we recognise our obligations in updating and expanding this program to meet the demands of the GDPR.

CaféX are dedicated to safeguarding the personal information under our remit and in developing a data protection regime that is effective, fit for purpose and demonstrates an understanding of, and appreciation for the new Regulation. Our preparation and objectives for GDPR compliance have been summarised in this statement and include the development and implementation of new data protection roles, policies, procedures, controls and measures to ensure maximum and ongoing compliance.

Please visit our compliance site to view the updated progress of our GDPR journey.

PCI-DSS

CaféX is PCI compliant: https://cafex.to/pcicert

EU-US Privacy Shield

We operate across the globe and serve customers in the United States and The European Union, CaféX is certified under The Department of Commerce EU-US Privacy Shield for the EU.

HIPAA

To comply with the requirements of HIPAA in the US, CaféX Communications executes a Business Associate Agreement (BAA) with HIPAA-covered entities in the Health and Medical services industry. The BAA certifies that CaféX Communications protects personal health information (PHI) in accordance with HIPAA guidelines. In support of the BAA, CaféX protects customer data in the following ways:

- Data-in-transit (e.g., the chat between a patient and the medical facility) is encrypted using TLS 1.2 with 128-bit AES encryption
- Data-at-rest (e.g., stored chat transcript) is encrypted using 192-bit AES

Note that customers cannot control the security keys being used to encrypt/decrypt data. This is done to ensure that security keys are not inadvertently exposed/revealed. Also, the keys used to encrypt the data-at-rest are broken up into multiple parts and each part is stored in a different location within the cloud solution.

This method of key storage prevents someone from hacking or accessing a single location and retrieving the key to decrypt an account's data.