FRAXION

Data security program

Fraxion Spend Management

Prime

T: 206-256-0771

600 1st Avenue
Suite 500E
Seattle, WA 98104

info@fraxion.biz
fraxion.biz

Table of contents

Organizational access control 3

- Control environment 3
- Access administration 3
- Personnel screening 3
- Security awareness and training 3
- Security incident reporting 4
- Sub processors and data transfer 4

Physical access control 4

- Physical protection of the data centers 4
- Availability 5
- Disaster recovery 5
- Fire detection and suppression 6
- Power 6
- Climate and temperature 6
- Monitoring 6

Technical security measures 6

- Database protection 6
- Application protection 7
- Encryption 7
- Intrusion protection 7
- Monitoring and review 8
- Malicious software protection 8
- Compliance certifications 8

Exclusions 9

Organizational access control

Control environment

Fraxion employees are required to sign a written acknowledgement form documenting their receipt and understanding of the employee handbook and their responsibility for adhering to the policies and procedures therein. Employees are also required to sign a confidentiality agreement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.

Access administration

Fraxion employees do not have direct access to Customer Data, except where necessary for Technical Support, system management, maintenance, backups and other purposes separately authorized by Customer in writing. Access to Customer Data is further restricted to technical and customer support staff on a need-to-know basis. When an employee or contractor no longer has a business need for these privileges, his or her access is revoked in a timely manner, even if he or she continues to be an employee or contractor of Fraxion. All access to Fraxion Azure Infrastructure requires a authorized named login account using multi-factor authentication (MFA) for access. All such access is logged and monitored, and account access rights are subject to both automatic monitoring and regular review for accuracy.

Personnel screening

Fraxion carries out an extensive interview process that spans multiple departments with possible candidates. Background verification includes prior work experience and personal references. Personal background checks may include, but are not limited to: credit checks, social media screening, and criminal record checks. Background checks are performed by a third-party service for employees with access to Customer Data as a component of the hiring process.

Security awareness and training

Fraxion maintains a security awareness program that includes appropriate training of Fraxion personnel on Fraxion's security policies. Training is conducted at the time of hire and periodically in accordance with the Fraxion Information Security Policy. Fraxion's Information Security Policy is reviewed periodically on a as needed basis. Any changes to the prior mentioned policy is reported to all employees and a receipt of acknowledgment is required.

Security incident reporting

Fraxion Employees are required to report any potential incident immediately to their Manager or Fraxion Infrastructure staff for review. Additionally, employees are encouraged identify potential improvements to security and surface them for review and possible implementation. Outside reports are accepted for review via the security@fraxion.biz email address. Both Fraxion and Microsoft Azure takes its obligations under the General Data Protection Regulation (GDPR) seriously. Microsoft Azure takes extensive security measures to protect against data breaches. These include both physical and logical security controls, as well as automated security processes, comprehensive information security and privacy policies, and security and privacy training for all personnel. Security is built into Microsoft Azure from the ground up, starting with the Security Development Life cycle, a mandatory development process that incorporates privacy-by-design and privacy-by-default methodologies. The guiding principle of Microsoft's security strategy is to "assume breach," which is an extension of the defense-in-depth strategy. By constantly challenging the security capabilities of Azure, Microsoft can stay ahead of emerging threats. For more information on Azure security, please review these resources.

Sub processors and data transfer

Fraxion may engage Sub processors and other Third-Party Suppliers (each as defined below) to perform some of its obligations under the Agreement. Fraxion shall ensure that Sub processors only access and use Customer Data in accordance with the terms of the Agreement and that they are bound by written obligations to protect Customer Data. At the written request of Customer, Fraxion shall provide additional information regarding Third Party Suppliers and their locations. Customer may send such requests to privacy@fraxion.biz. "Sub processors" means Fraxion affiliates and Third-Party Suppliers that have access to, and process, Customer Data. "Third Party Suppliers" means the third-party contractors and suppliers engaged by Fraxion for the purpose of processing Customer Data in the context of the provision of the Hosted Applications or Fraxion Platform. As part of providing the Hosted Applications or Fraxion Platform, Fraxion may transfer, store and process Customer Data in South Africa or any other country in which Fraxion and its Sub processors maintain facilities.

Physical access control

Physical protection of the data centers

Microsoft Azure designs, builds, and operates datacenters in a way that strictly controls physical access to the areas where your data is stored. Microsoft understands the importance of protecting your data,

and is committed to helping secure the datacenters that contain your data. Microsoft Azure has an entire division at Microsoft devoted to designing, building, and operating the physical facilities supporting Azure. This team is invested in maintaining state-of-the-art physical security.

Microsoft takes a layered approach to physical security, to reduce the risk of unauthorized users gaining physical access to data and the datacenter resources. Datacenters managed by Microsoft have extensive layers of protection: access approval at the facility's perimeter, at the building's perimeter, inside the building, and on the datacenter floor. Layers of physical security are:

Physical access to data centers is strictly controlled by the cloud infrastructure provider ("PaaS Provider", e.g., Microsoft Azure) both at the perimeter and at building ingress points by security staff. Authorized staff must pass a two-factor authentication to access data center floors which are monitored by cameras. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff. The PaaS Provider only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee or contractor no longer has a business need for these privileges, his or her access is immediately revoked, even if he or she continues to be an employee or contractor of the PaaS Provider. All physical access to data centers is logged and audited routinely.

Availability

Azure is globally organized into regions and each region is made up of several geographically distributed data centers. As outlined by Microsoft's Azures Service Level Agreement (SLA), commitments for uptime and connectivity for all clients are clearly stated in said agreement. All data centers are online and serving customers; no data center is "cold." Fraxion leverages Azure provided methods and infrastructure to prevent interruptions from individual data center or data center subsystem failure. The data centers have backup power and environmental protection systems, which are regularly maintained and tested. Fraxion also leverages multiple Azure regions to provide protection for failure of an entire region. These systems and their implementation is continually reviewed for potential improvements.

Disaster recovery

Each customer environment has one (1) master and at least one (1) slave instance that are mirrored continuously to one another. These instances of the Hosted Applications are located in physically separate data centers. Each Fraxion production instance is backed up on a regular interval at the PaaS Provider.

Fire detection and suppression

Automatic fire detection and suppression equipment has been installed to reduce risk and damage to data center environments.

Power

The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Data center facilities have power backup and environmental protection systems in the event of an electrical failure for critical and essential loads in the facility. Uninterruptible power supplies and vast banks of batteries ensure that electricity remains continuous if a short-term power disruption occurs. Emergency generators provide backup power for extended outages and planned maintenance. If a natural disaster occurs, the datacenter can use onsite fuel reserves. High-speed and robust fiber optic networks connect datacenters with other major hubs and internet users. Compute nodes host workloads closer to users to reduce latency, provide geo-redundancy, and increase overall service resiliency. Microsoft ensures high availability through advanced monitoring and incident response, service support, and backup failover capability. Geographically distributed Microsoft operations centers operate 24/7/365. The Azure network is one of the largest in the world. The fiber optic and content distribution network connects datacenters and edge nodes to ensure high performance and reliability.

Climate and temperature

Data centers are conditioned to maintain atmospheric conditions at optimal levels. Personnel and systems monitor and control temperature and humidity at appropriate levels.

Monitoring

The PaaS Provider monitors electrical, mechanical, and life support systems and equipment so that any issues are immediately identified. Preventative maintenance is performed to maintain the continued operability of equipment.

Technical security measures

Database protection

Database infrastructure is completely segregated from the Internet via firewalls and network and system level access controls. Applications have secure identity accounts for login, and no user access other than

administrative is granted. All connections to Azure SQL Database require encryption (TLS/SSL) at all times while data is "in transit" to and from the database. SQL Database uses TLS/SSL to authenticate servers and clients and then use it to encrypt messages between the authenticated parties. SQL Server and SQL Database support transparent data encryption. Transparent data encryption encrypts SQL Server and SQL Database data files, known as encryption data at rest. Transparent data encryption encrypts the storage of an entire database by using a symmetric key called the database encryption key. In SQL Database, the database encryption key is protected by a built-in server certificate. The built-in server certificate is unique for each SQL Database server

Application protection

Application infrastructure is completely segregated from the Internet via an application firewall and network and system level access controls. Traffic is monitored and assessed for malware, inappropriate call methods and protocols, call patterns and behaviors, and other threat assessments. Monitoring is continuous and real time with appropriate alerts on detection.

Encryption

Access to Fraxion's on-demand applications and services is only available through secure sessions (HTTPS) and only with an authenticated login and password. Passwords are never transmitted or stored in their original form. Azure supports various encryption models, including server-side encryption that uses service-managed keys, customer-managed keys in Key Vault, or customer-managed keys on customer-controlled hardware. With client-side encryption, you can manage and store keys on-premises or in another secure location. Data at rest in Azure Blob storage and Azure file shares can be encrypted in both server-side and client-side scenarios. Azure Storage Service Encryption (SSE) can automatically encrypt data before it is stored, and it automatically decrypts the data when you retrieve it. The process is completely transparent to users. Storage Service Encryption uses 256-bit Advanced Encryption Standard (AES) encryption, which is one of the strongest block ciphers available. AES handles encryption, decryption, and key management transparently.

Intrusion protection

The application infrastructure is protected against intrusion by industry standard firewall and access controls at the network, host, and application levels, and are reinforced by automated monitoring and detection systems. Fraxion conducts periodic internal testing of systems and services and regularly

employs independent third-party penetration testing and vulnerability scanning. Customer is prohibited from performing its own penetration testing on any system of Fraxion or its suppliers.

Monitoring and review

Automated monitoring and detection systems are deployed across all servers and services, leveraging advanced ML backed automated analysis and alerting tools. Specific events such as account creation or modification, infrastructure provisioning, or security systems access directly alert Fraxion infrastructure staff any time they occur for additional review. Security logs are reviewed on a regular basis for other events that require direct follow up by Fraxion staff.

Malicious software protection

Fraxion and the Microsoft Azure PaaS will ensure that the Hosted Applications and the Fraxion Platform include reasonably up-to-date versions of system security agent software which shall include reasonably current and tested malware protection, patches and anti-virus protection.

Compliance certifications

Fraxion's infrastructure resides on Azure public regions and utilizes Azure PaaS systems and services. Azure cloud services have one of the broadest sets of compliance certifications among public cloud providers, including: SOC 1 & 2, ISO 27001, ISO 9001, GDPR, and many others.

The following certifications have been generated against the Fraxion architecture as of July 2019 and are available upon request. SOC TSP Compliance, ISO 2700 Compliance and PCI DDS 3.2 Compliance. Penetration testing was carried out by Qualysis with no reported discrepancies Level 1-5. July 2019.

Fraxion regularly tests its applications against vulnerabilities and test for compliance, both at a infrastructure level and at an application level.

Azure SOC 1 Compliance	Last performed: 2019/06/30	Outcome: Compliant
Azure SOC 2 Compliance	Last performed: 2019/06/30	Outcome: Compliant
Azure SOC 3 Compliance	Last performed: 2019/06/30	Outcome: Compliant
SOC TSP Compliance Report	Last performed: 2019/07/03	Outcome: Fraxion environment is compliant with 12 of 12 supported SOC TSP controls

ISO 27001 Compliance Report	Last performed: 2019/07/03	Outcome: Fraxion environment is compliant with 7 of 7 supported ISO 27001 controls
PCI DSS 3.2 Compliance Report	Last performed: 2019/07/03	Outcome: Fraxion environment is compliant with 26 of 26 supported PCI DSS 3.2 controls
Qualsys Penetration Test	Last performed: 2019/07/12	Outcome: Fraxion environment has 0 L1-L5 security vulnerabilities

Exclusions

If Customer installs, uses, or enables third party services that interoperate with the Hosted Applications then the Hosted Applications may allow such third-party services to access, use, or otherwise process and transmit Customer Data. Fraxion's Security Program does not apply to any processing, storage, or transmission of any such Customer Data, and Fraxion is not responsible for the security practices (or any acts or omissions) of such third-party service providers with respect to data transmitted to and from such third-party services. The Security Program excludes: (i) data or information shared with Fraxion that is not stored in the applicable Fraxion Platform; (ii) data in Customer's virtual private network (VPN) or a third-party network other than one that is under a subcontract with Fraxion to assist Fraxion in fulfilling its obligations in the Agreement; or (iii) any data used, processed, stored or transmitted by Customer or Users in violation of this Agreement.