Jenzabar Information Security Program Summary

Purpose

This is a high-level overview of the Information Security Program at Jenzabar, Inc, headquartered at 101 Huntington Avenue, Suite 2200 in Boston, Massachusetts. This summary is not intended to list every element of our program, nor should it be deemed a representation, a warranty, or a covenant by Jenzabar. Certain details about our program are confidential, with some information shared with business partners and Clients under a signed non-disclosure agreement.

Values

We treat our customer information, and the personal information of our associates, as confidential. We employ appropriate technologies, policies, and procedures to protect our customers and staff and to uphold our legal responsibilities.

Data Protection

Our internal security program is designed to address the confidentiality, integrity, and availability of data in Jenzabar's care and is consistent with our privacy policy located at https://www.jenzabar.com/jenzabar-privacy-policy-0

Compliance and Governance

Our information security program is designed to be compliant with all applicable laws, regulations, and orders of national and local governments of customers in which we serve as well as compliant with certain standards. This includes the General Data Protection Regulation (GDPR) of the European Union, the Family Educational Rights and Privacy Act (FERPA), and Massachusetts Data Security Regulations under 201 CMR 17.

All datacenters that Jenzabar utilizes must meet the following minimum requirements:

- SOC1, SOC2, SOC3 Annual Reports (some public and some restricted access)
- Tier 3, or higher rated Datacenters
- ISO, PCI, HIPAA, FIPS and other certifications and compliance

For Clients using Jenzabar products on the IBM cloud, see https://www.ibm.com/cloud-computing/bluemix/compliance

For Client using Jenzabar products on Microsoft Azure, see https://azure.microsoft.com/en-us/overview/trusted-cloud/compliance/

For Clients using Jenzabar products on AWS, see https://aws.amazon.com/compliance/pci-data-privacy-protection-hipaa-socfedramp-faqs/

Jenzabar will not use a data center without having the appropriate written agreement in place with certain performance and protections set forth in writing, which Jenzabar will pass along to its Clients to the extent permitted by such agreements.

Our internal controls and practices are further informed by standards and publications such as NIST 800-61, the CIS Critical Security Controls and the Australian Signals Directorate Strategies to Mitigate Cyber Security Incidents.

Technology

We employ multiple layers of defenses that include the following:

Network

Well maintained physical and virtual firewalls to defend against internal threats and regulate network traffic. Jenzabar's internal corporate systems are isolated from applications provided through managed services. Inbound e-mail is protected by a leading security service to filter out phishing campaigns.

Endpoint

Jenzabar staff operate well patched workstations running industry standard anti-malware software.

A project is underway to regularly scan all endpoints to identify vulnerabilities, malware, and potential indicators of compromise (IOCs). We seek to routinely add defenses to our environment that detect/block malicious activity, thwart lateral movement of an attacker within our network, or detect/block exfiltration of data.

Encryption

Customer data is encrypted at rest on servers using AES256, and in transit with Transport Layer Security (TLS).

Physical Securiy

Access to all Jenzabar offices is restricted to authorized personnel only in buildings with on-site security staff.

Incident Response

Jenzabar has a documented Privacy and Security Incident Response Plan, which includes activation of an Incident Response Team (IRT) to cover potential or actual privacy or security incidents. The Director of Information Security leads the IRT to assess a potential incident, ensure remediation, and incorporate lessons learned from the experience into our information technology and security practices.

Awareness

We keep abreast of threats and security best practices through public and private information resources. Our internal security awareness program is presently being revised, but will include at least one mandatory annual training session, regular internal phishing assessments, and periodic email alerts.

Oversight

Program management is the responsibility of the Directory of Information Security, with oversight by the Chief Compliance Officer and the Information Security Committee. Additional oversight is provided by the company's senior management team and Board of Directors.

Questions

Questions about our information security program should be directed to the Director of Information Security via security@jenzabar.com

Updated: May 17, 2019