PURPOSE Enterprises, Inc. Security Policy

PURPOSE
ENTERPRISES, INC.

This document was last updated on April 28, 2020.

Contact: contact@purposehq.com

Overview

PURPOSE Enterprises Inc.'s security policy has multiple components and is formulated around a multilayered strategy with controls at multiple levels of data transfer, storage and access.

These components include:

- Corporate Security Policies
- Data Security
- Operational Security
- Physical and Environmental Security
- Regulatory Compliance

Corporate Security Policies

PURPOSE recognizes the importance and sensitive nature of the data that it is entrusted with. As such, PURPOSE is committed to the security of all information stored on its computer systems and its commitment is enshrined in the corporate code of conduct that all employees follow. In addition, all employees are screened with thorough background checks.

PURPOSE Enterprises, Inc. Security Policy

PURPOSE also has a set of security policies that cover the usage and access of sensitive data and credentials to accounts, computer and network systems, application services, change management, safe network usage, remote access, and a host of other IT resources. The PURPOSE Corporate Employee Handbook mandates that all employees agree with the PURPOSE Employee Security Guidelines, which includes policies such as the following:

- Employees are required to enable two-factor authentication in every internal and external service where two-factor authentication is made available.

- Employees must adhere to the PURPOSE Privacy Policy and are never allowed to communicate directly with any applicant or student without the expressed consent of the Customer.

Data Security & Data Integrity

PURPOSE has extensive policies and controls designed to protect client information. PURPOSE uses a distributed database to store information across a number of computers. Data in databases is also replicated across multiple computers in order to ensure that no single system is a single point of failure.

Application & Software Security

PURPOSE follows software industry best practices at every level of the application to ensure that data is retrieved, stored and transmitted securely.

Secure Network Transport with HTTPS

PURPOSE transmits all web application data to our employees and users via the HTTPS protocol. HTTPS is the industry standard for any service that transmits sensitive information via the web. Using HTTPS ensures that all data is encrypted while in transmission and only PURPOSE can decrypt the data upon arrival. Additionally, no malicious third-party agent can impersonate PURPOSE's service and intercept privileged request parameters.

Secure Information Retrieval

In all cases, PURPOSE only retrieves data specific and necessary for the purpose of building features that add direct value to the client.

Customer-Specific Logical Databases

Each business, school or district's data is stored in its own PURPOSE logical database with different authentication credentials from other customer databases. This ensures that one customer's data cannot be retrieved with credentials for another customer, either by an internal PURPOSE system or a PURPOSE client user.

Operational Security Personnel

All PURPOSE web, application, communication, and database servers are accessible only by background-checked PURPOSE staff. Only authorized

PURPOSE employees with the necessary operational responsibilities are allowed to access or modify network, database, application resources and settings. Employees have unique User IDs which are used to log into PURPOSE systems and have targeted permissions to view and manipulate systems information. Activities are logged for any required auditing.

Monitoring

PURPOSE takes system security very seriously and utilizes a number of tools to monitor access to its systems. All inbound and outbound requests made on PURPOSE's systems are logged for review by staff.

Infrastructure and Software Security

PURPOSE's infrastructure is built on technology that has been rigorously tested by the technology industry.

Network access is strictly controlled. All networked systems have access restricted to authorized personnel, and all non-public facing machines can only be accessed from within PURPOSE's private network.

- PURPOSE's infrastructure is built on top of the operating systems, databases and software provided by trusted commercial vendors and reputable open source projects.
- PURPOSE relies on many open source technologies that have been proven in the industry to be reliable and secure.
- PURPOSE's engineering team actively monitors industry security announcements for software bugs or exploits that may impact its operations.

Upon discovery of bugs or exploits, the engineering team will immediately apply the officially recommended software update to address the issue.

If you would like to report any concerns with PURPOSE's security practices or implementation, please email contact@purposehq.com.

Physical and Environmental Security

PURPOSE utilizes Amazon Web Services (AWS) to host and operate its private databases. AWS is highly regarded as one of the most secure and robust cloud service providers in the world. As an industry-leading cloud service provider, AWS has secure data centers equipped with nondescript facilities, professional security staff, controlled access, video surveillance, intrusion detection and other security features. This ensures that all data is separated from outside connections and access is limited to select, current members of the PURPOSE team.

If you would like to learn more about AWS security policies, click here.

Regulatory Compliance Family Educational Rights and Privacy Act (FERPA)

Given the sensitive nature of student and education data, PURPOSE understands that it is important to comply with the Federal FERPA regulation. Access to education data inside PURPOSE's systems is tightly controlled and requires explicit written permission from a school or district before we will begin transferring information from their systems.

Children's Online Privacy Protection Act (COPPA)

PURPOSE products and services are COPPA compliant. Because we take steps to ensure that schools and districts have given explicit permission at every step in the process of connecting them to PURPOSE. All PURPOSE education data has received consent for use. At PURPOSE, the security and privacy of student information is our topmost priority. PURPOSE is committed to ensuring that the information stored in its systems remains safe and secure.

It is this "security first" approach to development that enables schools to work with PURPOSE with absolute confidence. At PURPOSE, we routinely perform security and privacy audits to ensure that data is kept secure and private. With PURPOSE, schools can rest assured the integrity and security of their data will be maintained.

For more information about PURPOSE security, please contact contact@purposehq.com.