6-13-2018

Exhibit A: DATA SECURITY AND CONFIDENTIALITY AGREEMENT

# Buzz provides…

## Regular security updates:

Every week we update Buzz with our latest enhancements, bug fixes, and security improvements. To avoid disrupting customers, all updates from external services are tested by software and humans before rolling out.

## Secure data access:

Our API provides secure access to Buzz data over TLS.

## Authentication:

We support external identity providers (IdPs) for single sign-on (SSO) with CAS and SAML, so users can sign into one application and be automatically logged into Buzz without needing to re-enter credentials. This feature can help eliminate the need for teachers and students to have multiple credential sets.

## Physical security:

Buzz uses Amazon Web Services (AWS). AWS protects a global infrastructure of hardware, software, networking, and facilities, and is designed and managed around a variety of best practices and global security standards. AWS participates in various assurance programs, including FERPA, SOC1, and SOC 2, and is regularly independently audited (see https://aws.amazon.com/compliance for full details).

## Protocol and session security:

We use HTTPS for all external communication and encrypt all inbound and outbound traffic using 2048-bit TLS.

## Backup and recovery:

Buzz data is backed up every day. In the case of a disaster, data can be recovered from these backups. Backups are regularly tested.

## Software development process:

The Software development process includes test-driven development, automated tests, peer code reviews, continuous integration and deployment, and change control, all with a focus on quality and security.

## Business Continuity/Disaster Recovery:

Our backups are stored in a separate region. The region is tested semi-yearly so that we can restore services in that region in the event of a regional disaster in the primary region.

## Incident Response:

We have a documented incident response policy that we have used to manage past incidents successfully.

## Preventative controls:

- Agilix filters all corporate email through multiple vendors' anti-spam and anti-virus software before delivery.
- Multiple Internet Service Providers (ISPs) provide redundancy in the event of a security incident.
- Fault and failure tolerant design provides uninterrupted services in the event of component failure.
- Web services include a redundant boundary, DMZ firewalls, and load balancers to protect all information assets.
- A default "deny-all" firewall policy controls inbound and outbound traffic with only required IP addresses and ports open.
- Remote access to AWS management for production systems requires two-factor authentication to connect.
- All PII is encrypted at rest and in motion for external traffic.
- Agilix requires the use of encrypted file transfer services for all information sent by the client or returned to the client; Agilix uses FTP/S (SSL 2048-bit).
- Web services enforce redirection to HTTPS connectivity to validate the authenticity of the server and to protect the logon authentication process.
- HTTPS encryption enforces TLS 1.0 or greater.
- All Agilix web applications include input validation, output encoding and other OWASP top 10 best practices to protect against vulnerabilities.
- Our application is Penetration Tested yearly, and to date, we have had no actionable items come from the test.

- The API system allows for domain-level password policy enforcement allowing administrators to enforce any of the following password restrictions:
    - Minimum character count.
    - Minimum number of character classes.
    - Minimum time before allowing reuse of a previously-used password.
    - Maximum password age (force password to be changed periodically).
    - Number of times to allow incorrect passwords before locking out account.
    - Length of time to lockout account.
    - Length of time to retain records of login attempts.
- For our internal administrative accounts, we also detect the use of passwords that have been publicly leaked in security breaches.

## Administrative controls:

- Agilix performs background checks that cover: social security number verification; searches of the local and national sex offender registry search; and a criminal history search (i) in the national/federal databases, and (ii) for any state and county in which the individual has resided.
- Agilix trains all of our employees yearly on our corporate policies and security controls. Special training is reserved for those employees with access to our highest level of data (Customer PII).

## GDPR

We are considered a processor under the GDPR. Data controllers provide us with their policies and requirements to support processing data under the GDPR. Per our privacy policy, we will delete customer data upon authorized request. (See https://support.agilix.com/hc/en-us/articles/115005063386)

## We keep our security current:

The information in this document is accurate as of the listed date and is subject to change. We update our systems and processes as security needs grow and change. If you have any questions, contact us through https://agilix.com/contact-us.

15. Subcontractors. Service Provider shall require that any subcontractor or agent receiving CDI is authorized by the District to receive CDI and that the subcontractor or agent expressly agrees to be bound to the terms of this Data Agreement.

16. Modifications. Service Provider will not modify or change how CDI is collected, used or shared under the terms of this Data Agreement in any way without advance notice to and consent from the District.

17. Arizona Law. This Data Agreement is made in the State of Arizona and shall be interpreted by the laws of the State of Arizona. Any dispute arising out of or relating to this Data Agreement shall be brought in the Maricopa County Superior Court or the United States District Court, District of Arizona.

18. Cancellation. The District reserves all rights that it may have to cancel this Data Agreement for possible conflicts of interest under A.R.S. § 38-511, as amended.

19. Arbitration. To the extent permitted by A.R.S. §§12-1518 and 12-133, the parties agree to resolve any dispute arising out of this Agreement by arbitration.

20. Amendments. All references to provisions of statutes, codes and regulations include any and all amendments thereto.

21. Miscellaneous. The provisions of this Data Agreement shall survive the termination, cancellation or completion of all work, services, performance or obligations by Service Provider to the District. This Data Agreement shall be binding upon the parties hereto, their officers, employees and agents. Time is of the essence of this Data Agreement. Except as expressly modified by the provisions of this Data Agreement, any underlying agreement for goods or services shall continue in full force and effect. In the event any inconsistencies exist between the terms of this Data Agreement and any underlying agreement, this Data Agreement shall control.

**IN WITNESS WHEREOF,** the parties hereto have caused this Agreement to be duly executed by its authorized parties on its behalf.

**Scottsdale Unified School District #48**

By: ______________________

Title: Asst Supt, Secondary

Date: 9/30/19

**VENDOR NAME: Florida Virtual School**

By: ______________________

Title: Dr. Louis Algaze - President & CEO

Date: 9/30/19