Agilix data protection and security overview

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 deployment.

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, and is regularly independently audited (see https://aws.amazon.com/compliance for full details).

Protocol and session security

We use HTTPS for all communication and encrypt all inbound and outbound traffic using a minimum of TLS 1.0 with a 2048-bit private key.

Backup and recovery

Our backend infrastructure design includes redundant servers, database mirroring, and redundant file storage with automatic recovery from failure of any single system. Buzz data is also 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 AWS region (>100 miles away from the primary hosting center). Security settings prevent accidental deletion or modification of critical data files. Backups are tested semi-annually to ensure that the backup data is valid and we are able to restore service in the alternate region in the event of a disaster.

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.
- Network security policies also prevent internal traffic except between specifically configured systems and ports.
- Remote access to Agilix systems requires two-factor authentication to connect.
- All PII is encrypted both in motion and at rest.
- Agilix supports encrypted file transfer services for all information sent by the client or returned to the client; Agilix uses FTP/S.
- Web services enforce redirection of HTTPS connectivity to validate the authenticity of the server and to protect the logon authentication process.
- HTTPS encryption enforces TLS 1.0 or greater and uses a 2048-bit RSA certificate key.
- All Agilix web applications include input validation, output encoding and other OWASP top 10 best practices to protect against vulnerabilities.
- Client access to web reporting applications require authentication for access; the minimum standard for access includes:
    - All system users must have a unique user name.
    - Passwords must conform to the API-enforced password policy, which may require certain password lengths, numbers of character classes, etc.
    - Authorized users can be required via an automatic system expiration to change passwords every 90 days or as configured for client-required policy.
    - The systems masks passwords so that they do not appear on screen when entering them, or in system logs.

  - Passwords and related security-sensitive fields are salted and hashed using strong encryption.
  - Buzz may be configured to end user sessions end after a specified number of minutes of inactivity.

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 **Agilix Buzz Privacy Policy**).

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 Agilix.com.