Information Security Program

Activate Learning

Updated 01.11.2021

This document outlines the measures that Activate Learning undertakes to protect the privacy of student data, and the ways in which Activate Learning will respond in the event of a data breach.

Security Practices

Activate Learning takes user privacy and data security seriously. We use industry standard measures to safeguard personal information in its possession against loss, theft, unauthorized use, or disclosure. Steps taken to secure student data include the following:

- Any sensitive online information is transmitted over secure, encrypted channels via HTTPS. Sensitive information is not transmitted over email.
- All student data are stored on secure servers utilizing firewall technology and are only accessible via HTTPS and with proper authentication.
- If student data needs to be copied to a local machine for providing customer support, the data is always password protected, and is immediately deleted from the local machine upon completion of the support task.
- Activate Learning does not respond to third-party requests to share student information. If a school requests that student data should be sent to a third party, Activate Learning sends the data to the school and never directly to the third party.

Further measures are described in our Privacy Policy.

Personnel, Training and Review

- Activate Learning will conduct regular trainings (minimum annually) to inform employees of appropriate methods for securing student data and PII.
- Activate Learning will conduct internal audits (minimum annually) of security practices to ensure procedures are being followed and new risks are being addressed.
- The Chief Product Officer serves as the Security Officer and will maintain and supervise WISP implementation and performance.
- Violators of the information Security Policy will be subject to review by the CEO, and the Security Officer, and may be subject to dismissal.
- Terminated employees will have their access to all servers blocked by deactivating their usernames and passwords.
- These policies will be reviewed at a minimum annually.

Data Breach Response

In the event Activate Learning discovers or is notified of a data breach, we will, as required by applicable federal and state laws, investigate, take steps to mitigate the potential impact, provide notice of the breach to applicable agencies, and customers. However, despite our efforts, no security measures are perfect and we assume no responsibility for any breaches.

The Data Breach Response team consists of the Chief Product Officer (team leader), the Web/IT Specialist, the Manager of Programming and the Manager of Dev/Ops.

In the event of a data breach, Activate Learning will follow this process:

1. Validate the data breach, including whether it is a breach of PII and what type of incident occurred.
2. Once a breach has been validated, assign an incident manager to be responsible for the investigation to coordinate the response activities, create response documentation and manage the flow of information to the public about the breach.
3. Assemble incident response team with representatives from multiple departments, including IT, mgmt, etc.
4. Determine the status of the breach, prevent further unauthorized access and preserve evidence for investigation, and document mitigation efforts.
5. Determine whether to notify legal counsel or law enforcement
6. Notify any affected parties as appropriate. Note: some states may require notification within a specific number of days.

Step-by-step how we handle PII (student data):

If a district elects to roster students by uploading a CSV file to Activate Learning, the following procedures will apply.

Citrix Sharefile, which is FERPA compliant, is used for this upload process. Each student roster Excel spreadsheet will be kept in a password protected folder in Sharefile. Each teacher has their own password protected folder. They do not have access to any other folders in the district. The list of passwords for these folders are kept in a separate secure database, only accessible by AL staff.

1. Activate Learning creates a secure folder for the specific school or district in Sharefile.
2. Customer receives an email from our Support Staff describing:
    a. The data format needed (Excel spreadsheet which will be in the Sharefile folder for that school/district).
    b. The link of the secure Sharefile folder for downloading/uploading the spreadsheet, along with an initial password which they can change.
3. Customer has the option to provide usernames and passwords for teachers and students on the spreadsheet. Recommended password format is 8 characters, with at least one number, one capital letter and one lowercase letter.
4. Spreadsheet is uploaded to a secure folder by the customer.
5. Our Support Staff will download the Excel sheet to check for review and uploading into the IDE system.
6. Once the data has been uploaded, our Support Staff will make the updated sheet available to the teacher again in the previously created Sharefile folder. This is to address situations where changes are needed.

ALDP (Activate Learning Digital Platform) Backup and Security Strategy

The following is a brief technical outline of the backup and security strategy for the ALDP system.

ALDP runs on a cloud configuration built on top of Amazon Web Services (AWS). Proper use of this system provides inherent stability and security features. ALDP's fleet of web servers exists behind an elastic load balancer with autoscaling rules to cope with spikes in demand as well as server crashes. The database uses a Multi-AZ deployment with automated failover to provide robust access to data. All other user-generated assets are stored on S3 which, according to Amazon, provides 99.999999999% durability.

Access to all web servers is protected by key logins. Password logins are disabled. AWS's security group feature denies access to all but the needed whitelisted ports and IPs. The database server exists inside of a Virtual Private Cloud, and is only accessible via the web servers. It does not have a publicly accessible IP address.

Backups are multi-layered. The application code and servers are agnostic. They do not contain any user data. As such, they can be created and destroyed at will by autoscaling rules. Deployment scripts can provision new servers with code existing on S3. This code also exists inside of code repositories in other locations as well. AWS's database service provides daily snapshot backups of the database. Beyond this, we take secondary backups of the database on a daily basis. Other user data resides on S3, which is extremely durable. Again, this is backed up on a daily basis.

These backups utilize S3's "Vault Object Lock" compliance feature. This allows them to be retained for 90 days without the possibility of any user (including the root account holder of AWS) modifying them. It satisfies industry compliant WORM (Write-Once-Read-Many) archival storage within this time window, and cannot be circumvented.

Our programming team follows best practices. For production items, we use randomly generated passwords stored inside of password vaults. The only time we use non-random passwords are when customers request them.