GAME LEARNING SECURITY PRACTICES

Los Angeles Unified School District's security requirements below. These security requirements where passed June 2019.

Information Security Level 1

Access Control

1.Does your product have role-based access controls that segregate the work actions, privileges, and access to protected data of all system users (e.g. student, administrator, teacher, etc.)?

Yes

2.Can your product remove a user's privileges without having to delete their account and reset their password without knowing the password?

Yes

3.Do all company system administrator accounts with elevated access to protected data meet all of the following password requirements? If all system administrators use Multi-Factor Authentication (MFA), answer yes.

a. passwords contain at least 12 characters

b. passwords contain at least 1 number, 1 uppercase letter, and 1 special character

c. passwords cannot be the same as the previous 5 account passwords

d. can not contain any common dictionary words

e. maximum invalid password attempts cannot exceed 5

Yes

4.Does your product automatically lock a company system administrator's account after five or fewer consecutive failed attempts? If all system administrators use Multi-Factor Authentication (MFA), answer yes.

Yes

Cryptography

5.Are District passwords and data transmitted through web browsers encrypted in transit using TLS 1.2 protocol or greater?

Yes

6.Are all user account passwords salted and hashed when stored at rest?

Yes

Operations Security

7.If your product requires files to be installed on user computers, has it been successfully tested to operate in an environment where common anti-malware scanning technologies are implemented to remove malicious software?

n/a

8.Does your product automatically create backups of transactional data that can be restored with no more than 1 day of data loss?

Yes

9.Does your product have a mechanism to synchronize time between all networked resources in your application environment with an NTP server or other time protocol?

Yes

System Acquisition, Development and Maintenance

10.Does your product persistently track each user's session activity, except using IP session tracking, to ensure that users are uniquely identified for the variable duration of their use of your product?

Yes

11.Is your product's computer source code systematically examined during the development process to find common security vulnerabilities?

Yes

12.Are all the major system components of your product scanned for common vulnerabilities before releasing it to production for customer use (e.g. web server, database server, etc.)?

Yes

Information Security Level 2

1.Do you plan to transmit, collect, use, require or request Personally Identifiable Information (PII)?

Yes

2.Is your organization currently ISO 27001 Certified?

No

Information Security Policies

3.Do you have a set of internally published policies approved by your management that defines your approach to information security that are regularly reviewed?

Yes

Organization of Information Security

4.Do you manage information security through assigned segregated roles and responsibilities (e.g. Chief Information Security Officer, Network Administrator, Incident Handler, etc.)?

Yes

5.Does your organization provide a secure connection for teleworking employees with privileged access to protected District data (e.g. VPN)?

n/a

Human Resource Security

6.Are administrators, who are responsible for maintaining equipment that house protected District data, subject to a pre-employment background check?

Yes

7.Are employees, who will access or disclose protected District data, required to complete information privacy and security training annually?

Yes

Asset Management

8.Are you capable of complying with the data destruction methods as outlined in the District's data destruction policy BUL-6916? This bulletin may be accessed at http://achieve.lausd.net/BUL-6916.

Yes

Access Control

9.Is there a process for the timely revocation and granting of access rights for all user roles in your product?

Yes

10.Are administrator system user accounts regularly reviewed for removing unnecessary or unauthorized elevated access rights?

Yes

11.Are accountability, authentication, and authorization methods in place to restrict access to utility programs that are capable of overriding your product's system and application controls?

Yes

12.Does your product restrict users to a single application session that times out after 30 minutes of inactivity?

Yes

13.Do you have role-based controls to restrict access to your product's source code?

Yes

Cryptography

14.Does your product encrypt protected District data "at rest" on storage media using no less than 128-bit AES (e.g. files, laptops, servers, etc.)?

Yes

15.Is protected District data encrypted in transit between your application and your database server using no less than 128-bit AES?

Yes

16.Do you have a system for securely generating, distributing, storing, revoking, logging, and auditing encryption keys?

Yes

Physical and Environmental Security

17.Are offices, rooms, and facilities (that protect District data) physically secured with a minimum mortise lock, and are the keys securely managed?

Yes

18.Do you have a documented policy to limit the unauthorized removal of District data from your organization's premises?

Yes

Operations Security

19.Does your organization have formal procedures in place to identify, approve, and record significant changes to systems that process protected information?

Yes

20.Can your product automatically log authentication attempts, application events, security events, database events, and administrator commands issued by users with root system privileges?

Yes

21.Do you have anti-malware software installed and updated regularly on servers hosting District data?

Yes

22.Does your product automatically create and time-stamp audit records when changes occur in the following?

a. User access

b. User privileges

c. Database schema objects

Yes

23.Does your product have the ability to export audit and transactional records in a human readable file format for review and analysis?

Yes

24.Are audit logs retained for at least 90 days on storage media?

Yes

25.Are servers or equipment that house protected District data on a regular security patch schedule?

Yes

Communications Security

26.Does your organization restrict the use of unsecure and deprecated network connection protocols and services? (e.g. Telnet, WEP, SSL, SMB v1, etc.)

Yes

27.Is your product's application environment segregated from the Internet through the use of a stateful firewall to ensure that access to District data is protected?

Yes

Supplier Relationships

28.Do you regularly monitor sub-contractors who may be responsible for maintaining your product or have access to protected District data to ensure that they comply with District information security requirements and regulatory requirements?

Yes

Information Security Incident Management

29.Does your organization have formal procedures for monitoring, detecting, analyzing, and reporting of information security events and incidents?

Yes

Compliance

30.Does your product implement technical controls to ensure that the allowed number of LAUSD users do not exceed the maximum number of licenses permitted?

Yes