EVERFI

DATA SECURITY POLICY

Last Updated: March 2017

1. Overview

Information security is an integral part of the technology process at EverFi, and our engineering staff is committed to developing secure applications and maintaining an intrusion-free corporate environment.

2. Purpose

The purpose of this policy is to provide guidance for how data should be collected, transmitted, stored and accessed to ensure the highest amount of security possible.

3. Scope

This policy applies to all EverFi employees and companies who access EverFi data. This policy also applies to engineers and architects that design and develop any system that will handle EverFi data.

4. Policy

4.1 Data Collection

4.1.1 EverFi collects only the minimum amount of information needed to fulfill its educational mission and provide a quality user experience. Requests to collect additional data must be reviewed with executive oversight.

4.1.2 Collection of data for all minors must abide by current FERPA and COPPA guidelines. Extra care must be taken to not collect PII data for minors under the age of 13. It is EverFi's policy to not collect PII data about a minor even if FERPA or COPPA allow for it, unless its absolutely necessary

4.2 Cookies

4.2.1 EverFi uses cookies in its software. The use of cookies are only for functional operation of the software such as keeping a logged in user's session. Session cookies must be cryptographically signed and encrypted to prevent any tampering from outside sources. Even as such, session cookies must hold only opaque information such as record IDs and not any actual data from within the platform.

4.3 Data Sharing and Usage

4.3.1 The primary use of any data is for the functional operation of EverFi's platform. Data will be routinely loaded and displayed on webpages and downloaded reports. The logged in user must always be authorized to view this data.

4.3.2 Data can be shared with EverFi partners and customers. Data may only be shared with a partner or customer for whom it was collected for. Demographic information about a student at University A will not ever be shared with University B.

4.3.3 Survey data will only ever be shared in aggregate and only with the partner or customer it was collected for. Minimum sample sizes must also be enforced before providing aggregate survey results to a partner. If the sample size for the aggregate report being shared is below the pre-established minimum that the data must remain inaccessible. This is to mitigate the potential of identify the responses of an individual due to a small sample size.

4.3.4 EverFi may use the data it collects for the purposes of improving its platform and products. Such improvements may include identifying and approving course module abandonment rates.

4.3.5 EverFi may perform research about user's attitudes and behaviors across its platform. This research may only be done in aggregate on survey data. EverFi will never view the responses or behaviors of individual users.

4.3.6 EverFi will never share user lists or email with anyone beyond the partner, and will not contact users without the permission of the partner. It should be noted that the EverFi platform does have the ability to send emails (for example, if we collect an email address at registration, we send a "Welcome Email" from EverFi that contains a reminder link to the learning portal). It should also be noted that EverFi provides technical customer support, and if a user contacts us for help, we may email or call them to resolve their technical issue.

4.4 Data Access Controls

4.4.1 Access to any form of data is on an as needed basis only. Only designated senior level engineers may have access to the databases that hold the platform's data. This includes any systems or consoles that may access the data and are not part of the normal end user software.

4.4.2 Copies of any system databases may never be made for any purpose other than backup retention or migration to an equally secure database. All database backups must adhere to the same access controls as the source database. All authorized copies of a database must be securely deleted as soon as they are no longer needed. This policy forbids the download of production level data for the purposes of debugging issues locally on an engineer's computer.

4.5 Data Storage and Transport

4.5.1 All data must be encrypted during transmission. This includes to and from the user agent of an end user, between EverFi applications and to and from the databases themselves. Where technology allows, all connections to any database must be through and encrypted means and must follow EverFi's Acceptable Encryption Guidelines.

4.5.2 All data at rest must be encrypted where technology allows. For relational databases this should be block level encryption performed at the hard disk to prevent access to the data in the event that a hard drive itself was stolen. This policy also applies to all snapshots and backup copies of the data.

4.5.3 All data transmission must remain within the private network of the platform. All systems handling data must be located on this network and behind a firewall with no access from outside the network. Exceptions are data transmitted via Http to an authenticated user agent, in which case the transmission of the data must follow the Data Sharing guidelines in section 4.3

5. Policy Compliance

5.1 Compliance Measurement

The EverFi Information Security team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the EverFi Security Committee in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.