EMMERSION

Emmersion Security Statement

Overview

Data Privacy Policy

The current version of the Emmersion privacy policy is publicly available online:
https://truenorthtest.com/privacy-policy/

Information Security Personnel

While hiring a dedicated CISO is on the roadmap, these responsibilities fall to our Chief Technology Officer at this time.

Business Continuity & Disaster Recovery Plan

At this time, Emmersion only has lightweight BCP and DRP documents. We are working continually on improvements. With a geographically distributed workforce and Cloud-hosted product, the risk of disruption due to external forces has been assessed as low or very low. Strategies for maintaining communication, product availability, and business continuity are continuously tested as staff members take advantage of work-from-home policies.
Despite these mitigating circumstances, development of a BCP document is underway.
Despite these mitigating circumstances, development of a DRP document is underway.

Minimum Requirements for using the Application

The Emmersion application is web-based, so clients only need to install a supported browser as specified in the support documentation: https://truenorthtest.com/troubleshooting/#browsers-and-devices

An optional API integration is also available. Documentation for that API can be found at
https://api.truenorthtest.com

Security Awareness

In addition to a security awareness primer as part of onboarding training, responses to security concerns are shared across the company generally as they arise.

Product development team members participate in a regularly scheduled (weekly) training program which includes security awareness training on OWASP recommendations, NIST standards, etc.

Certification and Audit

As a small but steadily growing technology start-up, Emmersion has yet to undergo an official IT auditing process or obtain specific certifications. At this point, Emmersion has an internal security scorecard for self evaluation based on the OWASP recommendations.
In addition, Emmersion applications are hosted at Microsoft Azure and receive weekly Azure Security Center updates for the resources in our subscription. The Security Center provides a Regulatory Compliance review of our infrastructure. Reports include `Azure CIS 1.1.0`, `PCI DSS 3.2.1`, `ISO 27001`, and `SOC TSP`. The results of these reports can be made available upon request.

> Under each applicable compliance control is the set of assessments run by Security Center that are associated with that control. If they are all green, it means those assessments are currently passing; this does not ensure you are fully compliant with that control. Furthermore, not all controls for any particular regulation are covered by Security Center assessments, and therefore this report is only a partial view of your overall compliance status.

FERPA Standards Compliance

Emmersion complies with this standard.

> Responsibilities of Third-Party Service Providers under FERPA
> These records include, but are not limited to, transcripts, class lists, student course schedules, health records, student financial information, and student disciplinary records. It is important to note that any of these records maintained by a third party acting on behalf of a school or district are also considered education records.
>
> When schools and districts outsource institutional services or functions, FERPA permits the disclosure of PII from education records to contractors, consultants, volunteers, or other third parties provided that the outside party
>
> 1. performs an institutional service or function for which the agency or institution would otherwise use employees;
> 2. has been determined to meet the criteria set forth in the school's or district's annual notification of FERPA rights for being a school official with a legitimate educational interest in the education records;
> 3. is under the direct control of the agency or institution with respect to the use and maintenance of education records; and
> 4. uses education records only for authorized purposes and may not re-disclose PII from education records to other parties, unless the provider has specific authorization from the school or district to do so and it is otherwise permitted by FERPA.

PCI Standards Compliance

Emmersion complies with this standard by delegating the handling of payment cards to Stripe for all in-product payment processing.This feature is further restricted to use by a small subset of clients due to legacy agreements. Stripe is certified to PCI Service Provider Level 1.

ISO 27001 Certification

Emmersion is not yet certified compliant with ISO 27001 though obtaining this certification is a priority on the security roadmap, and controls are being implemented in preparation for engaging an external auditing firm. Microsoft Azure Security Center provides a Regulatory Compliance review of Emmersion infrastructure with regard to ISO 27001 compliance and all recommendations are being implemented incrementally.SSAE 16 /

SOC 2 Type 2 Certification

Emmersion is not currently SOC 2 certified nor have SSAE 16 audits been performed.
Microsoft Azure provides a SOC 2 Type II Report for the cloud services in use.
NIST Cybersecurity Framework
Emmersion is adopting the NIST framework through continual improvements to our product and processes.

FISMA Standard

The FISMA Implementation Project includes several key security standards and guidelines including FIPS and NIST Special Publications. Emmersion is adopting the NIST security framework.

Application Security

User Authentication

The web-based Emmersion application uses cookie-based authentication with 2-hour sessions. Signing out of the application terminates all active sessions for that user (not just the current session).

While MFA options and single-sign on options are not currently available, the client API allows administrators to create automatic sign-in links for test takers to create a SSO-like experience. These links are single-use, expire after 5 minutes, and cannot be created for administrators.

Password policy and handling

The Emmersion product password policy is based on the NIST 800-63B Digital Identity Guidelines Section 5. Specifically, each password must be **at least 8 characters** (though no longer than 256 characters). Passwords may not contain the username for the account and may not contain the words “webcape” nor “truenorth”. Additionally, passwords on the top 10,000 most-frequently-used passwords list recommended by OWASP are not permitted.
All user generated passwords are salted and hashed using an irreversible cryptographic hash (bcrypt). Only the secure hash result is stored.
Multiple consecutive authentication failures do not yet trigger automatic account lockout. This feature is on the roadmap.

Role-based access control

All client users have one of two roles. They are either account administrators or test takers.This role cannot be altered after user account creation.

Account administrators have access to client data including limited PII, detailed and aggregate reports, and can grant access to test takers either individually or in bulk.

Test takers have access to assigned assessments and personal reports only. They have no access to any PII other than their own and no administrative rights to the system.

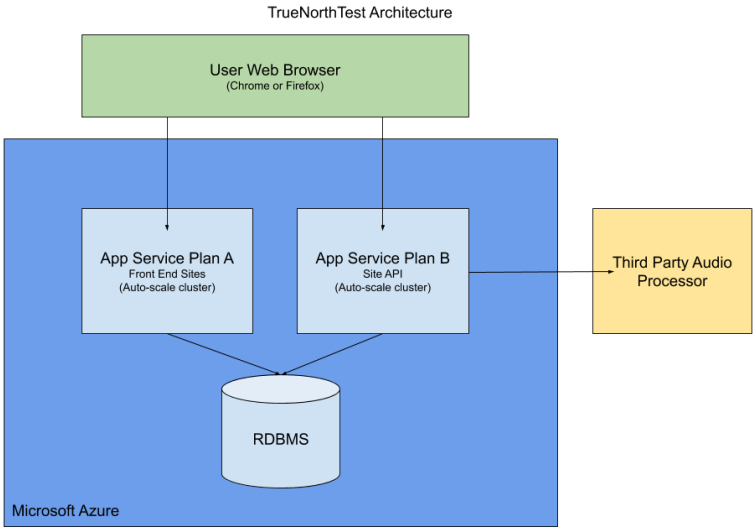
Input validation and error messages

The Emmersion application observes OWASP security guidelines regarding input validation and data sanitization to prevent security risks and ensure data integrity. Error messages are likewise scrutinized to secure against risks such as exposed stack traces or leaking information.

Application Architecture

System Architecture

The Emmersion application is delivered as a web application. Client interactions are through HTTP; primarily in a web browser. Direct API interaction is also through TLS 1.2 secured HTTP.
After initial registration, all user interactions require authentication.



Multi-tenant architecture and access controls

The Emmersion application is implemented with physical and logical multi-tenancy. Client data rows are identified with a unique client identifier and/or a unique user identifier.

- Client administrators associated with that client ID may retrieve and update data for that client including users, assessments, and score reports.
- Test Takers may only retrieve and update data associated with their user ID.
- Emmersion Learning administrators may manage data for multiple clients.

Data Loss Prevention

Account administrators have the option to download CSV reports or query data from our API. No other document or data sharing features exist in our system.

User Access / Application Audit Logs

Audit reports of performed administrator actions are not currently available, but are on the roadmap.

Application web logs

The Emmersion application is hosted in Microsoft Azure provided infrastructure which provides HTTP metrics and application logging. This may include event data and client IP addresses. This data is not made accessible to clients. These logs have a 90 day retention period.

Data Handling

Data Breaches

Emmersion has had no significant data breaches since the company founding in 2015.
In the event that significant data breach is detected, affected clients will be notified via email immediately after determining the scope of the breach and restoring reasonable system integrity.

Data Zone

The Emmersion application is a cloud-hosted application that runs in Microsoft Azure data centers within the United States. Server and database backups are stored in the Azure Storage Accounts also within the United States.

These data centers include:

- **Central US** located in Iowa
- **North Central US** located in Illinois
- **West US** located in California
- **West US 2** located in Washington

Data at Rest

All client data is stored in Microsoft Azure SQL Server and/or Microsoft Azure Storage. Both of these repositories encrypt data at rest.
Per Azure documentation for Azure SQL Server:

> *Transparent data encryption (TDE) helps protect Azure SQL Database, Azure SQL Managed Instance, and Azure Data Warehouse against the threat of malicious offline activity by encrypting data at rest.*
> *...*
> *In Azure, the default setting for transparent data encryption is that the database encryption key is protected by a built-in server certificate. The built-in server certificate is unique for each server and the encryption algorithm used is AES 256.*

Per Azure documentation for Azure Storage:

> *Data in Azure Storage is encrypted and decrypted transparently using 256-bit AES encryption, one of the strongest block ciphers available, and is FIPS 140-2 compliant. Azure Storage encryption is similar to BitLocker encryption on Windows.*

Data in Motion

Connections to the Emmersion web application servers require TLS 1.2 for all requests. Connections to Azure SQL Server require TLS 1.2 as well.

Data Retention

All client data is retained for the duration of any active contract and indefinitely after the completion of all contracts. Upon receipt of a written request and within 30 calendar days, a copy of client data can be provided. Upon receipt of a written request and within 30 calendar days, client data can be deleted from our systems or anonymized if it is of an essential nature to our business operations.

Data Backup

All Azure SQL Server data is backed up using Azure read-access geo-redundant storage. These backups are all encrypted using the same TDE technology described in the **Data at rest** section. Backups are retained for approximately 2 years.

Third Parties

Third-party providers are evaluated based on need and risk. The CTO acting as CISO evaluates the risk profile of vendors by reviewing the details of the data sharing requirements, service level agreements, privacy policies, security certifications, data regulation compliance, etc. prior to introduction into the company operations or the product.

Access to Client Data due to use of the product

In accordance with the Emmersion privacy policy, no personally identifiable information (PII) is transferred to third parties without prior notification and consent of the client.
Emmersion products rely on third-party providers for data processing of non-PII data as follows:

- Microsoft Azure - Cloud Hosting provider for SaaS products. Client information is stored there as described elsewhere in this document.
- Carnegie Speech - This automated speech recognition provider processes anonymous audio files with no PII attached.
- IBM Watson Speech to Text - This automated speech recognition provider processes anonymous audio files with no PII attached.

- Google Cloud Speech API - This automated speech recognition provider processes anonymous audio files with no PII attached.
- MailGun - Email sending tool that retains a record of transactional emails.

Access to Client Data as part of business operations

- Salesforce - This CRM tool tracks client data related to opportunities, sales, contracts, marketing automation, etc.
- Quickbooks - This accounting software manages company finances including client invoices and client details.
- G Suite - These communication and productivity tools ensure smooth operation of Emmersion. Client information is found in files in Google Drive and emails in Gmail.
- FreshDesk - Customer Success tool that stores information related to support requests.

Change Management

Software Development Lifecycle

The Product Development teams at Emmersion follow a Lean software development process similar to an Agile process, but with more emphasis on short iterations and limiting work in process. This reduces lead time for feature delivery and updates. See also https://en.wikipedia.org/wiki/Lean_software_development

This process requires that several roles be filled:

- **Product Manager:** sets the priority of work items in alignment with strategic goals
- **Team Architect**: ensures technical implementations meet security, quality, performance, and system design goals and ensures deployment methods, infrastructure, and site reliability meet our standards
- **Software Engineer**: implements, tests, reviews software features and performs automated and manual testing of delivered features
- **User Experience Designer**: performs user/usability research and ensures UI meets accessibility standards and our internal consistency requirements

Production software and infrastructure changes made by each Product Development team are:

- Approved by the **Product Manager** or **Team Architect**
- Reviewed by at least two **Software Engineers** through collaborative development (aka pair programming or mob programming) or through pull requests in the source control management system
- Validated through automated and manual processes in the staging environment prior to release to the production environment
- Validated in the production environment

Change Management Process

The CMP is built into the Lean software development lifecycle. Changes are prioritized by a Product Manager or Team Architect. The cross-functional development team collaborates on implementation and verification. All changes made to production systems require peer review. Updates occur at a rapid cadence measured in hours and days rather than weeks or months.

Software and System Patches

Hardware and software vulnerability patches managed automatically as a feature of the Platform as a Service features of Microsoft Azure.
Software package dependencies (e.g. packages sourced from npm or nuget) are reviewed monthly. Packages with identified vulnerabilities are updated, tested, and deployed through the standard SDLC process.
The Emmersion internal security scorecard is reviewed quarterly. Any issues identified at this time are prioritized and resolved through the standard SDLC process.

Client Notification

The Emmersion Client Success team communicates major changes, including changes which could affect client security, with all clients, working directly with any that have specific needs or concerns.

Emergency Change Authorization

Emergency changes receive front-of-line privileges and are expedited but otherwise follow the standard SDLC process. The small batch sizes of the Lean Software development lifecycle not only make this possible, but also the most rational course of action.

Remote access of customer data

The Emmersion workforce is distributed with many employees working from home full time in roles including sales, engineering, and marketing. These employees have access to the customer data necessary to perform their job functions often through SaaS tools such as Salesforce, Google Suite, and our product administration tool. Hard-drive encryption using standards-compliant operating system features is required for all computers used outside of the office.

As the Emmersion application is cloud-hosted and developed by a distributed Product Development team, engineers have remote access to client data in the production database. Firewalls restrict incoming data store connections to known locations (IP addresses) and firewall rule changes are logged. All connections to data

stores are protected by TLS 1.2 or better. Access is logged automatically by our cloud provider and alerts are raised when suspicious access is detected. A VPN solution is being developed.

Network Security

As a cloud-based SaaS product company, Emmersion has no application or storage servers located physically in the office. Wired connections are preferred for office staff workstations. Wireless network is secured using WPA2 (shared key) standard.

The Emmersion application deployment relies on security features of Azure including Network Security Groups (with restrictive firewall rules) and Security Center Monitoring and Alerting (including adaptive network hardening, just in time access controls, and suspicious activity alerting). These controls run continuously and retain alert logs for 30 days. Firewall changes must be approved by a member of the Technology Leadership Team.

The product networking configuration is migrating iteratively to the following target design:

* This is a convention not enforced by an Azure resource