Torii Security White Paper

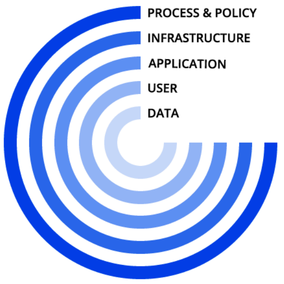
Last updated: May 28, 2018

Introduction

Torii puts high focus and effort on keeping our customers' data safe. Our customers put their trust on us and we take this responsibility seriously.
This document highlights Torii's security standard and practices, aimed to ensure data confidentiality, integrity and availability. Torii's security standards and practices are a multi-layered approach to incorporates best practices for preventing security breaches.

Standards

Torii follows the ISO 27001 standard..



Multi-layered security

Application Security

General

Torii development team is trained on OWASP Secure Coding Practices and uses industry best practices for building secure web apps.

Encryption

All data is encrypted both in transit and at rest. Database instances, including read replicas and backups are encrypted using the industry standard AES-256 encryption algorithm. Encryption is enforced via TLS to all data in transit. The databases are hosted on Amazon RDS in the US regions using a Multi-AZ deployment for enhanced availability and durability.
Only secure (HTTPS) access to Torii website and app is allowed. Non-secure HTTP requests are first redirected for the HTTPS endpoint before they can be served.

Role Based Access Control (RBAC)

Torii is built as single page app, with a Rest API backend server. Several scopes exist to restrict the API access in these level: anonymous, user-scope, organization scope. Each user is identified with a unique session, stored in a secure, HTTPS only, session cookie. The user scope is set in the database. Each request to the API server is first checked for the right scope in order to validate that a user is allowed to invoke the API.
All API requests are scoped to the minimal required permission.

Multi Tenancy

Each Torii customer’s data is hosted in Torii’s shared infrastructure and segregated logically by Torii application.

Authentication

User Authentication and Passwords

Torii authenticates all users with a unique ID and password. All Torii user passwords are encrypted and salted. Access to Torii restricted API resources are always authenticated.

SAML & MFA Authentication

Torii supports SAML 2.0 authentication, allowing customers to implement Single-Sign-On (SSO) with their own access policies, including whitelisting and multi-factor authentication (MFA). Customers may also integrate user authentication with their own policy store (E.g. Active Directory).

Infrastructure Security

Cloud Computing Services

Torii infrastructure relies on these services:

- Amazon API Gateway
- Amazon Aurora Database
- AWS Lambda
- Amazon Route 53 DNS
- Netlify (CDN)

Production Access

Access to production data and server is restricted to a named list of employees. The list is owned and maintained by the VP Engineering.

Security Patches

Torii maintains no physical or virtual servers. All services are consumed as Infrastructure-as-a-Service (IaaS) by Amazon AWS and Netlify (CDN). Amazon and Netlify perform automatic security patches.

Backups

To maintain a robust disaster recovery strategy, Torii leverages Aurora automated backups which allows us secure backups as well as quick recovery.
We test our backup recovery regularly.

Operational Security

Process & Policy

Torii's security is first and foremost a mindset and training all Torii employees adhere too. On top of that, there are several several security policies in place:

1. Internal password policy
2. Information security policy
3. Information security risk management policy
4. Security incident response policy

Change Control

All changes to Torii application and systems goes through a format change control process in order to minimize the risk associated with such change. The process enables tracking of changes made to the systems and verifies that risks have been assessed, inter-dependencies are explored, and necessary policies and procedures have been considered and applied before any change is authorized.
All changes are being reviewed by at least another employee, before the change takes effect.

End Notes

Here at Torii, protecting our customer's data assets is of high priority. We continue to tighten and enforce our security standards across policies, procedure, technology and people.
We want our customer to be rest assures their data is protected by our approach.
We welcome further questions and clarification.
Don't hesitate to contact us at security@toriihq.com