Last Updated: April 2025

Initus Security Policy

Overview

At Initus Technologies Inc. (Initus), the security and integrity of our platforms and user data are of the highest priority. We implement a robust set of modern security practices across all our solutions to protect against unauthorized access, data breaches, and cyber threats. This policy outlines the specific security measures employed across the Initus platform and its associated applications. A Platforms/Solutions Security Summary can be found in Appendix A.

Security Measures

1. Secure Database Access (AWS VPC-Restricted Firewall)

Database access is tightly controlled through an IP-restricted firewall within AWS's Virtual Private Cloud (VPC), ensuring only authorized internal systems can connect.

- ✅ Platforms/Solutions: Initus Platform Authentication Layer, MigrateEase, CodeQuilt, InitusGPT, InitusIO, Audiolize, Textualize, Capsulize

---

2. Short-Lived Access Tokens (JWT)

Authentication tokens have a short lifespan, minimizing the risk of unauthorized access due to token leaks or credential theft.

- ✅ Platform: Initus Platform Authentication Layer

---

3. Secure Token Storage (Browser-Protected Cookies)

Tokens are encrypted and securely stored in browser-protected cookies to reduce risk from browser extensions or malicious scripts.

- ✅ Platforms: Initus Platform User Interface, Initus Platform Authentication Layer

---

4. Enterprise-Grade SQL Injection Protection (ORM)

Our database framework has built-in defenses against SQL injection, ensuring data integrity and compliance with industry security standards.

- ✅ Platforms/Solutions: Initus Platform Authentication Layer, CodeQuilt, InitusGPT, InitusIO, Audiolize, Textualize, Capsulize

- ⛔ Platform not covered: Regarding **MigrateEase**, additional SQL-injection safeguards are unnecessary. The data it handles is strictly **read-only** and has already passed through our centralized sanitization and validation layers before exposure. For Data Visualization projects no write operations are permitted, the component presents no viable vector for injection attacks, so omitting it from the covered platforms does not affect our overall security position.

---

5. Cross-Site Request Forgery (CSRF) Prevention

CSRF protection prevents unauthorized transactions or actions executed on behalf of authenticated users.

- ✅ Platforms/Solutions: Initus Platform Authentication Layer, MigrateEase, CodeQuilt, InitusGPT, InitusIO, Audiolize, Textualize, Capsulize

---

6. Seamless & Secure Authentication (OAuth2 with Google & Microsoft)

Supports secure Single Sign-On (SSO) through OAuth2, enabling frictionless and secure login via trusted identity providers.

- ✅ Platforms: Initus Platform User Interface, Initus Platform Authentication Layer

---

7. Strong Password Encryption

User passwords are stored using advanced encryption techniques, ensuring protection against credential compromise.

- ✅ Platform: Initus Platform Authentication Layer

---

8. Comprehensive Security Logging & Monitoring

We track user actions, API requests, IP addresses, and geolocation to ensure full visibility for audits, compliance, and proactive threat detection.

- ✅ Platforms/Solutions: Initus Platform Authentication Layer, CodeQuilt, InitusGPT, InitusIO, Audiolize, Textualize, Capsulize

---

Initus is committed to the ongoing evaluation and strengthening of our security practices. This policy reflects our dedication to industry best practices and continuous improvement in safeguarding our clients' platforms and data.

For further information or questions about our security policies, please contact:

Security Policy Team

INITUS TECHNOLOGIES INC.

5473 Blair Rd., Suite 100-90706

Dallas, TX 75231

info@initus.io

Appendix A: Platforms/Solutions Security Summary

Security Measure	Security Measure Description	Initus Platform User Interface	Initus Platform Authentication Layer	MigrateEase	CodeQuilt	InitusGPT	InitusIO	Audiolize	Textualize	Capsulize
Secure Database Access (AWS VPC-Restricted Firewall)	Database access is tightly controlled through an IP-restricted firewall within AWS's Virtual Private Cloud (VPC), ensuring only authorized internal systems can connect.	☐	☑	☑	☑	☑	☑	☑	☑	☑
Short-Lived Access Tokens (JWT)	Authentication tokens have a short lifespan, minimizing the risk of unauthorized access due to token leaks or credential theft.	☐	☑	☐	☐	☐	☐	☐	☐	☐
Secure Token Storage (Browser-Protected Cookies)	Tokens are encrypt stored in secure cookies, preventing unauthorized access by browser extensions or malicious scripts, enhancing protection against cyber threats.	☑	☑	☐	☐	☐	☐	☐	☐	☐
Enterprise-Grade SQL Injection Protection (ORM)	Our database framework has built-in defenses against SQL injection, ensuring data integrity and compliance with industry security standards.	☐	☑	☐	☑	☑	☑	☑	☑	☑
Cross-Site Request Forgery (CSRF) Prevention	CSRF protection is in place to prevent unauthorized transactions or actions from being executed on behalf of authenticated users.	☐	☑	☑	☑	☑	☑	☑	☑	☑
Seamless & Secure Authentication (OAuth2 with Google & Microsoft)	Supports secure single sign-on (SSO) through OAuth2, enabling frictionless login via trusted identity providers (Google and Microsoft).	☑	☑	☐	☐	☐	☐	☐	☐	☐
Strong Password Encryption	User passwords are stored using advanced encryption techniques, ensuring compliance with security best practices and protecting against credential compromise.	☐	☑	☐	☐	☐	☐	☐	☐	☐
Comprehensive Security Logging & Monitoring	Tracks user actions, API requests, IP addresses, and locations, ensuring full visibility for security audits, compliance, and proactive threat detection.	☐	☑	☐	☑	☑	☑	☑	☑	☑