Zydaptive

# Security Practices

Last Updated: April, 2023

867 Boylston Street
5th Floor
Boston, MA 02116

# POLICY

The security and privacy of our customers take precedence.  We never share any information about our customers or their clients with any third party, period.

**Development Practices:**

At Zydaptive, we take a security-first approach when it comes to our software and business practices. All employees at Zydaptive are well-versed in security best practices and participate in security training at regular intervals. This includes annual training on the OWASP Top 10.

**SDLC:**

Our Secure Software Development Lifecycle (SDLC) introduces security testing into every development stage, from design through coding, testing, and beyond.  At the beginning of each written feature, we review our security posture and determine the security measures required to move forward with the feature.  Because we employ a security-first approach, we're able to identify security requirements ahead of time and introduce the appropriate security measures, along with automated testing to validate them.

**Static Code Analysis:**

Every software developer at Zydaptive writes code in an environment that provides built-in security awareness and advice with each keystroke taken. We also employ full static analysis of our codebase within every build. This helps to identify security concerns early on. Putting security best practices early in the development phase allows us to mitigate security risks and bugs ahead of time. This gives us greater confidence in providing a secure platform to our customers.

# POLICY

**Technology:**
The Zydaptive platform leverages a role-based architecture, allowing you secure access to private information, track version history, review audit logs, and more.

**Cloud Access:**
All Zydaptive instances reside behind AWS WAF (Web Application Firewall), configured to monitor traffic and block attacks.

Work with your Zydaptive implementation consultant to lock down instance access to specific geographic areas or specific IP addresses so you control who can log in and from where.

**MFA Everywhere:**
All Zydaptive instances require Multi-Factor Authentication out of the box. Using MFA provides a necessary level of security in today's security landscape. Anytime someone logs into the application, they must enter a secondary authentication code which can be delivered to their desktop or phone.

**3rd Party Application Review / Penetration Testing:**
We work with industry-leading security consultants who review, test, and simulate attacks via penetration testing on our platform annually.

# POLICY

## Login Security:

Zydaptive Login:  We use industry-standard bcrypt hashing for passwords, with an auto-scaled cost factor ensuring that our hashing algorithm is current with today's technology.

We employ password-strength policies consistent with today's best practices to ensure your account logins remain safe.

Single Sign On (SSO) / Multi-Factor Authentication (MFA): We support both single sign-on and Multi-Factor Authentication for secure login.

All login session activity is recorded and monitored, along with the IP addresses of associated login activity.  We employ auto-lockout policies which block accounts after certain failed login attempt criteria are met.

# POLICY

**Encryption:**

In Transit:

At Zydaptive, we encrypt all data in transit all the time. Data is encrypted between public endpoints and the application as well as within the application's local private networks. All in-transit data is encrypted with current TLS protocols. Two industry-leading providers, Amazon and Let's Encrypt, issue our certificates.

At Rest:

All data on the Zydaptive platform is encrypted at rest:

- All Cloud Storage is encrypted at the storage layer using AES-256.
- All databases utilize an encrypted storage engine that leverages AES-256 to encrypt all files the database uses. This encryption extends not only to the current data but also to all backups that we maintain to ensure the continuity of our services.

Application Level:

Within the Zydaptive platform, the most sensitive fields are encrypted at the application level before persisting to the database using military-grade 256-bit encryption. Because our platform has many business use cases, consult with your platform integration admin to determine which fields we encrypt at the application level. Customer encryption keys are securely held and managed via AWS Key Management Service.

# POLICY

**Document Storage:**
All documents stored on the Zydaptive platform are encrypted with military-grade 256-bit technology and stored on an encrypted, private S3 storage medium.

**Service Continuity:**
Our platform is hosted within Amazon Web Services and spread across multiple availability zones. This is to ensure that the service is always available when you need it. Our databases are clustered across availability zones, and all use a minimum of three nodes that can self-heal via automatic failover.

We utilize continuous database backups and automated snapshots which guarantee Point in Time recovery, should that be required. Backups are stored in the highly durable AWS S3 storage service and are encrypted both at the file level, as well as the storage layer.

Michael Goldsmith
Michael Goldsmith
CEO at Zydaptive

Zydaptive