SECURITY AT LAPTIS

www.laptis.io
Date of last update: 6/28/2025

At Laptis, we streamline access to trusted substance use treatment. Protecting our customers' data and privacy is core to everything we do. Below is an overview of our security practices:

Organizational Security.

We follow industry best practices to ensure high standards for data privacy and security. Our team members undergo security awareness training covering topics such as phishing prevention and password management.

Third-Party Audits and Penetration Testing.

We engage independent third parties to perform annual penetration tests to validate and strengthen our security posture.

Cloud Security.

All Laptis services are hosted on **Amazon Web Services (AWS)** in the **United States**. AWS maintains robust security certifications. For more details, visit AWS Security.

All data is **encrypted at rest and in transit (TLS/SSL)** to protect against unauthorized access.
We perform vulnerability scanning, maintain audit logging and monitoring, and utilize backup and disaster recovery processes to ensure service continuity.

Access Security.

Access to our cloud infrastructure and sensitive tools is limited to authorized team members who require it for their role. We enforce **Single Sign-On (SSO), two-factor authentication (2FA), strong password policies,** and **least privilege access controls**. We also perform **quarterly access reviews** to maintain appropriate permissions.

Incident Response.

We have a documented **incident response plan** with escalation procedures to rapidly identify, mitigate, and communicate security incidents.

Vendor and Risk Management.

We perform **vendor security assessments** before engaging new vendors and conduct **annual risk assessments** to identify and address potential threats.

Contact Us.

If you have any questions, comments, or concerns, or wish to report a potential security issue, please contact **security@laptis.io**.