TransnetYX®
tick@lab

IT Security in tick@lab: Protecting Your Research Data with Enterprise-Grade Measures

Andreas Staubi, 20-Oct-2025

Introduction

Data security is not a feature—it is a fundamental requirement for modern SaaS solutions, especially in biomedical research where sensitive project information and intellectual property are at stake. a-tune recognizes that research institutions, pharmaceutical companies, contract research organizations, and government agencies entrust us with their most valuable asset: their data.

tick@lab is built on a security-first architecture that combines industry best practices, rigorous compliance frameworks, and continuous operational vigilance. As an ISO 27001 certified organization, we don't just meet industry standards—we continuously evolve our security posture to address emerging threats. This white paper provides decision-makers and IT professionals with an overview of the comprehensive security measures we implement to protect your research data and ensure confidentiality, integrity, and availability.

Security Governance and Management

Effective IT security begins with organizational commitment and structured processes. a-tune maintains an established Information Security Management System (ISMS) aligned with ISO 27001 standards. Regular audits—both internal and external—ensure that our security controls remain effective and that security is an integral part of how we design, develop, and operate tick@lab.

All employees participate in regular IT security awareness training, ensuring that human factors are addressed systematically. Security considerations are integrated into every phase of tick@lab development: from design through coding and testing. We maintain established incident response and management processes that ensure immediate notification to affected customers without delay, enabling transparent crisis management. Regular tabletop exercises and disaster recovery drills validate that our plans work in practice, demonstrating our commitment to maintaining service availability and data integrity.

Infrastructure Security and Data Protection

tick@lab operates on Amazon Web Services (AWS), leveraging a globally distributed infrastructure that combines reliability with geographic flexibility. For customers with specific regulatory or sovereignty requirements, we offer deployment on AWS GovCloud.

Single-Tenant Architecture: Unlike multi-tenant solutions, each tick@lab customer receives a dedicated application instance with separate processes, ensuring logical isolation from all other customers. While our infrastructure may span shared AWS resources for efficiency, your data is strictly separated at the application and data storage levels—each customer maintains separate database schemas. This architectural choice significantly reduces the attack surface and ensures that even in the unlikely event of a security incident affecting one customer, other customers' data and processes remain completely unaffected.

Network Security: Enterprise-grade firewalls protect all tick@lab environments, with only TLS-encrypted traffic permitted to the internet. All other access vectors are completely isolated from external networks. Production environments are strictly separated from a-tune's corporate network, creating an additional security boundary that protects customer data even if internal systems are compromised.

Encryption: All data is encrypted both in transit and at rest. Communication with tick@lab occurs over current TLS-encrypted connections, protecting data as it moves between users and our servers. All stored data—including databases, file systems, and backups—is encrypted using AWS encryption services with keys managed through AWS Key Management Service (KMS) and appropriate access controls.

Backups and Disaster Recovery: tick@lab implements a multi-layered backup strategy with regular automated backups stored on AWS S3, off-site copies replicated to geographically separate AWS regions, and retention policies aligned with customer requirements. Regular recovery testing verifies integrity and ensures rapid recovery capabilities under any circumstance.

Monitoring, Threat Detection, and Vulnerability Management

tick@lab benefits from 24/7 monitoring of both application performance and underlying infrastructure through a managed Security Operations Center (SOC) as a Service.

Our dedicated operations team, distributed across three time zones, provides round-the-clock support capability. Automated alerting systems enable rapid detection and response to any anomalies or security events, ensuring threats are identified and investigated immediately, regardless of time zone.

Proactive vulnerability management is continuous. We conduct regular security scanning to identify potential weaknesses before they can be exploited and engage independent security professionals to perform comprehensive penetration testing on a regular basis. These controlled assessments simulate real-world attack scenarios and validate that our defenses are effective. Comprehensive anti-virus and anti-malware solutions provide real-time protection against known threats. When vulnerabilities are identified, they are prioritized based on risk and remediated according to defined service level objectives, with critical vulnerabilities receiving immediate attention.

Data Ownership and Customer Control

A unique aspect of tick@lab security is the clarity of data ownership: you own your data. a-tune does not store passwords—tick@lab integrates directly with your organization's authentication systems, allowing you to maintain control over user access through your own identity management systems. This eliminates an entire class of security risk while ensuring access control remains under your authority.

You determine what data is captured within tick@lab and for how long it is retained. Your data is never used for purposes beyond providing the tick@lab service. This customer-centric model aligns with modern data protection regulations such as GDPR and reflects broader principles of responsible data stewardship.

Secure Development and Personnel Security

Security begins at the design phase. tick@lab is developed using secure coding practices, security requirements, code reviews with security focus, and static and dynamic application security testing integrated throughout the software development lifecycle. This "security by design" approach ensures security is woven into tick@lab from the beginning, not bolted on as an afterthought.

Conclusion

tick@lab's multi-layered security approach—grounded in ISO 27001 compliance, single-tenant architecture, cloud-based infrastructure resilience, comprehensive encryption, continuous monitoring, and customer data ownership—provides the assurance that your biomedical research data is protected by enterprise-grade measures.

We understand that trust is earned through consistent action and transparency.
We continuously invest in our security program, adapting to new threats and evolving requirements. For specific details about how tick@lab security features support your compliance requirements or to discuss your unique security needs, please contact our security team.