How LabLynx Meets a State Security Mandate With Support From TrustNet

The state's information security standard mandates an independent third-party security audit at least annually. TrustNet has been the independent auditor for that obligation since 2021.

Client: One state government client

August 24, 2026 · 3 min read

IN BRIEF

For LabLynx's work with one state government client, an independent third-party security audit is not optional. The state's information security standard mandates it, every year. LabLynx engaged TrustNet as its independent auditor for this obligation, and TrustNet has held this engagement since 2021.

At a glance

SECTOR	State government
REQUIREMENT	An independent third-party security audit, at least annually
CLIENT	One state government client
STANDARD	The NIST Cybersecurity Framework and the NIST SP 800-53 control catalog
AUDITOR	TrustNet, an IT security and compliance firm
ENGAGEMENT SINCE	2021
REMEDIATION CLOCK	30 days for the most serious findings

Key takeaways

- The state's information security standard applies to vendors who operate IT systems containing state data, and mandates an independent third-party security audit at least annually.
- The standard is grounded in the NIST Cybersecurity Framework and built on the NIST SP 800-53 control catalog.
- Every finding receives a risk rating with a remediation deadline tied to severity, 30 days for the most serious.
- LabLynx prepares a corrective action plan within 15 business days and reports progress to the state quarterly.
- LabLynx does not route every deployment through the same audit; the engagement covers the state deployment specifically.

Labs hand LabLynx some of their most sensitive data: patient results under HIPAA, evidentiary records in forensic and medical examiner work, and program data for state agencies. Those labs are right to ask how that data is protected and whether anyone independent has checked. For LabLynx's work with one state government client, that check is not optional. The state's information security standard mandates it, every year.

The standard

The standard applies to vendors who operate IT systems containing state data. It is grounded in the NIST Cybersecurity Framework and built on the NIST SP 800-53 control catalog, whose twenty control families cover everything from access control and audit logging to incident response, contingency planning, and supply chain risk. Vendors subject to the standard must undergo an independent third-party security audit at least annually.

The auditor

LabLynx engaged TrustNet, an IT security and compliance firm, as its independent auditor for this obligation, and TrustNet has held this engagement since 2021. Independence is a requirement of the state's audit rules, not a courtesy: TrustNet performs no management functions, prohibited non-attest services, or other

services for LabLynx that would compromise its position as an independent examiner.

What gets examined

Each annual cycle, TrustNet reviews the LIMS application for a state government client, management's review of the controls for the cloud hosting environment, and the organizational security controls behind it: the policies, training, incident response program, change and patch management, and backup and recovery procedures that operate behind the software. The technical work includes vulnerability scanning, penetration testing, configuration review against NIST benchmarks, and validation that access controls and audit logging hold up under examination.

Findings do not get filed away

Every finding receives a risk rating with a remediation deadline tied to severity, 30 days for the most serious. LabLynx prepares a corrective action plan within 15 business days, reports progress to the state quarterly, and TrustNet's managed security services independently re-tests the most serious findings before they can be closed. The audit is a cycle that must be completed, evidenced, and verified, then started again the following year.

What this means if your lab runs on LabLynx

This engagement covers the state deployment specifically; LabLynx does not route every deployment through the same audit. What carries across is the organizational security program that the audit examines, the policies, training, incident response, and vulnerability management that operate behind every LabLynx deployment. So when a lab asks how its data is protected, part of the answer is that the controls behind the platform have stood up to an independent auditor's annual review.

> *TrustNet has been a dependable partner for LabLynx since 2021. Their support runs smoothly in the background, the process has become increasingly seamless over time, and the reporting continues to meet our needs. We value working with a team that does what it is supposed to do without creating unnecessary issues, and that has been our experience with TrustNet.*
>
> **Laurie Mueller**
>
> COO, LabLynx

Where this could go for your lab

If your lab operates under its own security or compliance requirements, this is also a picture of how the two of us are linked and what that could mean for you. LabLynx has direct experience deploying under a strict, independently audited standard. TrustNet provides independent security and compliance auditing for organizations directly. If you need a configurable LIMS, talk to us; if you also need an independent audit of your own environment, TrustNet does that work, and you have just seen how the two of us work together. Schedule a 30-minute scoping call to walk through your LIMS needs, and learn more about TrustNet at trustnetinc.com.

The partner

PARTNER

TrustNet

An IT security and compliance firm.

www.trustnetinc.com