LabLynx Security

At LabLynx, our security plan is currently based on NIST 800-53 v4. We must comply with HIPAA as a business associate for many clients. State privacy programs apply for clients with privacy laws, such as NY and CA. Security and privacy controls are maintained such that our clients are capable of complying with their many security, privacy, and laboratory standards, frameworks and regulations.

We have a cross-organizational committee that meets regularly on cybersecurity issues. We ensure policy training during onboarding, policy issuance, and randomized security tests. All LabLynx organizations, departments, and activities are responsible for ensuring that their programs are in compliance with LabLynx policies. Organizations must actively monitor management practices and controls, and take remedial action when significant deficiencies are encountered or improvements needed. We keep our server operating systems up to date with scheduled maintenance tasks, weekly reviews for vulnerabilities and periodic reviews of infrastructure.

This document describes the overall LabLynx security plan and can be used when evaluating the security of your supply chain for a LIMS. The hosted applications such as ELab are designed to be configurable to comply with your specific security requirements. Clients are capable of making many such configurations such as, but not limited to: users and profiles, access controls such as password complexity and history, session length, login info banners, and auditing of user account changes.

Amazon Web Services

LabLynx hosts at Amazon Web Services (AWS) where all physical infrastructure and physical security are second to none; you can view the AWS SOC 3 report here.

LabLynx uses the AWS network for User Authentication, Network Security, VPS IaaS, PaaS, and all customer data is isolated with limited access. Development boxes are maintained at AWS.

The global information system infrastructure resources and services provided by AWS are located in the US and other AWS countries where applicable.

AWS offers FedRAMP compliant services (AWS US East-West).

LabLynx

https://aws.amazon.com/compliance/data-center/controls/
https://d1.awsstatic.com/whitepapers/compliance/AWS_SOC3.pdf
https://aws.amazon.com/about-aws/global-infrastructure/regions_az/
https://aws.amazon.com/compliance/fedramp/

LabLynx Privacy and Cybersecurity Policies

You can view our privacy statement here and privacy within client applica
utilize the client privacy statements and links.

Information Security

LabLynx's information security standard governs the security, protection, and handling of LabLynx information and records, and defines four broad information security classifications:

Internal: Data is made available to internal company personnel as appropriate for their role.
Public: Data is freely available to the public.
Confidential: Access to data requires special qualifications or is covered by legal agreements. Examples include PII, PHI, the "special" GDPR categories, PCI-regulated data, data covered by NDAs, and so on.
Restricted: Data that could lead to irreparable harm, criminal charges, or similar if accessed without Authorization.

Access to data must be restricted to users or information systems with a legitimate business need and authorized by the data owner or an authorized delegate of the owner. Authorization is on a need-to-know basis. Access is restricted to performing a specific job task. This requires that access is permissible to only the data, programs, or portions of the operating system to perform assigned functions or explicitly required for system functionality. Systems shall be configured to enforce access privileges based on job classification and function.

Encryption

Data at rest will be encrypted for all systems of moderate or higher risk impact and will be considered for systems of low impact.
All data in transit will be encrypted with modern algorithms appropriate to the software. For web traffic, this is currently TLS version 1.2 or higher.

Data Sharing & Retention

LabLynx holds all client electronic data and records for at least 6 years unless directed otherwise. Clients can request adherence to their internal retention policy. Clients are responsible for providing such a policy upon agreement between both parties. LabLynx is responsible for data and records of clients that are hosted and maintained on LabLynx servers.

LabLynx Policies

Change Management Policy
Access Control Policy
Configuration Management Policy
Data Management Policy
Development Integration and Maintenance Policy
End-User Messaging Policy
End-User Computing Policy
Malicious Software Policy
Password Control Policy
Information Security Policy
Laptop Encryption Policy
Log Management Policy
Problem and Incident Management Policy Server and Host Security Policy
Separation of Duties Policy
Incident Response Plan
Third Party Services Policy
Disaster Recovery Policy

LabLynx Privacy and Cybersecurity Policies

Access and Single Sign On

LabLynx offers single sign-on (SSO) via SAML. OpenSocial is built by LabLynx with the intention of handling SSO via SAML. For each organization that utilizes OpenSocial based SSO, a new instance of the application is created, manageable by the client.

Access to the hosted network is provided to personnel only on an as needed basis, only on approved devices.

Access to company resources is provided using the same secured technologies and, in many cases, the same applications, that we make available to our hosted clients via web-enabled technologies. Access to the LabLynx networks via remote access is controlled using VPN or encrypted SDWAN software with authentication to OpenSocial password authentication.

Our organization's assets are formally inventoried and classified and our critical assets are identified. We keep an inventory of authorized devices and software. We reduce and control administrative privileges on all assets. Access privileges to information assets must go under semi-annual review to ensure authorities granted are required.

Personal Health Information (PHI)

PHI data is often hosted on behalf of our clients, and is regulated under HIPAA (Health Insurance Portability and Accountability Act), for which compliance is a legal obligation. LabLynx is a Business Associate, not a Covered Entity, under HIPAA.

The company is responsible for providing appropriate security and maintaining privacy for data hosted and stored on behalf of covered entities, or other HIPAA business associates.

Non-production environments with PII data should never leave the hosted, protected network, even to approved, connected devices. For example, developers must not copy a LIMS database or application files for such a site onto a local device. It must remain on servers provided for this purpose within the network to protect PII used in production and non-production environments against unauthorized release or exposure, consistent with controls in the production environment.

Security Assessments

Monitoring

LabLynx conducts regular security assessments, security audits, and internal risk assessments of the information systems. The company also finds potential risks posed to the information system from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, and outsourcing entities). LabLynx conducts regular vulnerability assessments of the information systems. LabLynx employs vulnerability scanning tools that allow the list of vulnerabilities tested to be automatically updated.

We monitor for unauthorized personnel, connections, devices, and software using Alienvault USM that tracks logins and connections. The LIMS also provides successful and failed login information. Asset reviews are done every 30 days.

AlienVault USM SIEM agents scan for vulnerabilities on all systems at least once per week.

There are no wireless networks associated with the sensitive networks. A variety of periodic audits, including remote access, are performed.

Incident Response

Our formal incident response policy and procedures are as follows: An Incident Response Team quickly reacts to computer-related incidents such as virus infections, hacker attempts, break-ins, unauthorized disclosure of confidential information, system service interruptions, breaches of personal information, and other security events. The Incident Response Team subscribes to various security industry alert services to keep abreast of relevant threats, vulnerabilities, or alerts from actual incidents.

DevOps will serve as a central point of contact for reporting any suspected or confirmed breach of personal information on an individual. After documenting the facts presented and verifying a suspected privacy breach occurred, DevOps will open a Priority Incident Request.

Clients are provided help desk accounts, for which all ticket creation and updates are emailed to the clients. We may also directly call, or email outside of the ticketing system, if the situation warrants.

LabLynx

866-522-5969 | sales@LabLynx.com | LabLynx.com

Disaster Recovery & Business Continuity

We take regular backups of all production environments with AWS, which are synchronized to multiple data centers in the AWS region. Backups are kept for 10 weeks. Backups are encrypted. All environments are scanned for malware, viruses, and other malicious code.

Each part of the DRP is tested annually for effective operation and successful information system operation at the selected disaster recovery site. Alternate recovery sites are maintained in case of major disaster. Clients can request disaster recovery testing in the Project Plan as a Planning Milestone in compliance with a contract between the customer and LabLynx Inc.

The hosted network is physically and logically isolated from all remote locations, including the company offices. It is hosted with AWS, for which personnel, guests, or otherwise, have no physical access. Damage to central offices or any other remote site will not impede continued work from other locations.

An estimated RTO time frame is based on one (1) hour per 100GB of restored data plus one (1) hour system configuration.

Server Instance Disaster: A server instance disaster would require restoring the destroyed server into a new instance at AWS from the most recent backup.

VPC/Network Disaster: A VPC/Network disaster would require restoring the destroyed VPC from the CloudFormation template backup.

AWS Availability Zone Disaster: A disaster event for an AWS availability zone would require restoring the destroyed environment into the alternate, functional AWS region.