Security Policy v4.7 (rev. 10/30/2018)

The security of the services we provide to our clients is paramount to our Clients and to Us. We provide mission-critical services for our clients and guard these services against interruption and misuse. We receive, store and manage data that is restricted from disclosure. We secure these data using the same measures we use to protect our own information. Longsight implements security by design (hardened systems; authenticated and encrypted access only) as well as security by default (all options are set to private unless explicitly set otherwise). This document defines the policies that guide Longsight's principles and practices for providing secure services.

1. Data access

    1.1. General

        1.1.1. Data access is limited to Longsight employees with a "need to know." Access to Confidential Information is limited to Longsight employees and contractors, and access to Covered Content is limited to Longsight employees only

        1.1.2. Longsight confidentiality agreements require all Longsight employees and contractors to protect Your Confidential Information and Your Covered Content from all unauthorized exposure as part of Our terms of employment.

        1.1.3. You will maintain accurate authentication and authorization data to control Your Users' access to the Services. We are not responsible for the security of Your authentication services or Your passwords that are compromised outside of systems controlled by Us.

        1.1.4. All Client data are stored at Amazon Web Services (AWS) regional data centers in the United States, unless otherwise specified in client agreements. Longsight follows AWS Security Best Practices.

    1.2. Physical access

        1.2.1. Physical access to the AWS data centers at which the Services are hosted is strictly controlled by AWS, following the AWS Security Best Practices. Only AWS employees have physical access; Longsight employees do not have physical access to the AWS data centers at which the Services are operated.

1.3. Virtual access

1.3.1. Longsight Employees have only virtual access to Your data and Services. All exchanges of your data, including all network connections to Longsight employees, take place using encrypting protocols over secure network connections. All endpoints (Ours and Yours) must maintain current certificates. Only under exceptional circumstances will Longsight employees store or transport any client data on secured, company- provided mobile devices (laptops). If such storage is needed, data shall be stored for as little time as possible and always encrypted in transport and at rest and password protected. Any exceptions must be reported immediately to Longsight management.

1.3.2. Longsight employees' access to your services is managed through a centralized LDAP authentication service. This provides a single point of management for Longsight staff access as well as convenience so that staff can follow strict credentialing requirements in the Longsight Employee Handbook which must be accepted as part of the Longsight terms of employment.

1.3.3. Access to your data of all types will end immediately upon termination of employment with Longsight.

1.3.4. Our email and shared document services are hosted by Google Apps for Business, access to which requires two-factor authentication. Our operational file store is encrypted in transit and at rest.

2. Security standards

2.1. Our computers and systems including those used by Longsight employees (which are managed centrally by Longsight) in the conduct of their work are protected by acceptable industry practices for antivirus, firewalls, and network and system intrusion detections systems.

2.2. All systems used in the storage, processing, transmittal and display of Your data must have operating systems that are current in release, with all unneeded services disabled, with default administrator access shut off, and with all critical security patches updated within 24 hours after the release of the patch.

2.3. We conduct routine event monitoring, promptly investigate suspicious incidents and respond accordingly.

2.4. SOC1-2-3 audit certifications are conducted annually on the AWS infrastructure that Longsight uses. All SOC1, SOC2 and SOC3 reports are available online.

2.5. We conduct routine security assessments for vulnerabilities (buffer overflows, open ports, unnecessary services, input filtering, cross site scripting vulnerabilities, SQL injection vulnerabilities, and any other well-known vulnerabilities). identified issues will be fixed or mitigated within thirty (30) days of the report.

2.6. Clients may not conduct security scans on Sakai instances hosted by Longsight without permission.

2.7. All Longsight services that send or receive Your Confidential Information or Your Covered Content must utilize appropriate encryption methods (SSL, sFTP, VPN, etc.). All network connections to Longsight must be encrypted. Clear text transactions are not permitted.

3. Changes to the policy

3.1. This policy may be updated from time to time. Updates will become effective as soon as they are published at www.longsight.com If there are any material changes to these policies, active clients will be notified by email prior to the change becoming effective. Your continued use of Longsight Services constitutes Your agreement to be bound by such changes to the policy. Your only remedy, if you do not accept the updated terms of a Longsight policy, is to discontinue use of Longsight Services.

4. Definitions

4.1. Confidential Information means the information that you have provided to us as part of the contracting or purchasing process. By example, this would include names, addresses, email addresses, phone numbers, account numbers, purchase orders, and other information that is not included in Your Covered Content. Confidential Information would also include the terms and pricing of the Longsight Service under this Agreement, Your Covered Content and all information clearly identified as confidential at the time of its disclosure.
4.2. Your Covered Content means all Longsight service data that You, Your agents or your end users provide to us as part of the use of Longsight's Sakai services. By example, this may include, among other data, the student name or identifier, student email address, student submissions, course names, grades, comments and annotations that may be associated with a student or instructor.
4.3. Us, We, Our and related terms means the company named Longsight, Inc. who developed and hosts the services, as represented by Longsight Employees.
4.4. Longsight Employees are US citizens serving as full-time, salaried employees of Longsight, Inc. for whom a background check has been completed, and who have signed the Longsight Employees' Handbook which requires adherence to security practices and includes a strict confidentiality agreement.
4.5. You, Your and related terms means the subscribing entity and all affiliated personnel who use the Longsight Sakai service. By example, You would mean the college, school district, university or company whose agents and end users access Longsight Sakai services.
4.6. Client means any organization or individual with whom Longsight has an active agreement for services.

Questions about this Security Policy should be directed to information@longsight.com.