Logmore security summary

Security is one of Logmore’s top priorities. Enabling data collection without unsecure USB connections is just the beginning, your data is always safe at Logmore.

Description of data flow

Sensor data

Logmore’s QR data loggers collect data into internal memory from sensors at set interval or based on set rules. The stored data is directly read from the calibrated sensors.

Data synchronization

Data that is stored in the logger’s internal memory can be synced to the web service by scanning the QR code seen on logger’s screen and by opening the link QR code contains.

Data is compressed and encrypted into the link. Data contained in the link can only be decrypted with secret encryption keys that are stored securely in the web service database.

Data presentation in user interface and API

The data stored in the secure database can be presented at Logmore Cloud user interface or API.
To receive the data user must be authenticated and authorized to access the data. Unauthorized person or client can’t read any information from the system.

Data validity

To ensure data validity several methods are used. These methods together make sure all data within the system is real data measured by the sensor and that the data has not been altered at any point of data flow within the Logmore system.

Encrypted incoming data

All data coming into the web service from logger devices is encrypted and all connections to Logmore Cloud are secure encrypted HTTPS-connections. Data can’t be altered by editing the incoming data without encryption keys.

Logger device encryption

Encryption keys are unique for every logger device. Encryption method used to ensure security of the data in the loggers is aes128-cbc. Encryption keys are stored securely in the web service database.

Data validity in web service database

Once data is received into the web service from logger device the inbound data block is automatically decrypted, decompressed and validated.

Measurement data that is received into the system can not be edited or altered by users in any way.
To ensure measurement data and authorization information security in the communication between user or client and web service the user interface and API always force encrypted HTTPS-connections for all users and clients consuming the data.

Logmore security summary

Web service infrastructure

The computation, storage and internet connection resources used to run the web service are acquired to Logmore from Amazon Web Services (AWS).

To ensure data persistence in extreme cases where whole AWS becomes unreliable, system is backing up all data every night to another 3rd party data center.

All the best security practices are used system wide to minimize security risks involved running system that's components are communicating through internet.

System is constantly monitored to prevent and notice performance issues, anomalies, invalid data or attacks.

Authentication

Users or system clients consuming data or user interfaces provided by web service are always authenticated through Auth0 identity provider platform. Authentication is ISO27001, ISO27018 compliant with HIPAA BAA and EU-US Privacy Shield Framework and has achieved a Level 2 audit Gold CSA Star certification for its cloud service security capabilities

Security and quality

Best development practices are used when developing the software to ensure the security and quality. System is constantly improving and every change is thoroughly tested to make sure the system has no security vulnerabilities or quality issues.

Logmore's operational staff are monitoring the system around the clock and each person has been trained to act upon any issues occurring in the system.