# Data Protection & IT Security Policy

Last modified: 22. September 2023

## 1. Purpose

The primary objective of LifeX's  Data & IT Security Policy is to increase employee and user awareness on potential cyber risks and cyber security procedures and to avoid accidental breaches, loss of confidential data and damages on operating systems . It outlines the concrete requirements and procedures in place.

## 2. Scope

This policy applies to all client data, personal data, economic data and other sensitive and confidential company data. Therefore, it applies to every server, database and IT system that handles such data, including any device that is regularly used for email, web access or other work-related tasks. Every user who interacts with LifeX's software systems and services is subject to this policy.

## 3. Policy

### 3.1 General

A. Each employee at LifeX as well as external clients of LifeX proprietary software systems will be identified by a unique user ID so that individuals can be held accountable for their actions.

B. The use of shared identities is not permitted.

C. Each user shall read this data security policy.

D. LifeX shall always provide all employees, users and contracted third parties with access to the information they need to carry out their responsibilities as effectively and efficiently as possible.

### 3.2 Access Control Authorization

A. Access to LifeX proprietary software systems will be given through the provision of a unique user account and complex password.

B. Logins to LifeX proprietary software systems are always logged. Records of user access may be used to provide evidence for security incident investigations.

C. Organisational accounts can only be  provided by LifeX's Product Team;

   a. For internal LifeX staff account access will be given based on records in LifeX's HR department.
   b. Account access for external clients of lifeX's proprietary softwares systems will be given based on clear instructions from the client's contact person and can only happen if a signed software service contract and data processing agreement is in place between LifeX and the client.

D. Access shall always be granted based on the principle of least privilege, which means that each program and user will be granted the fewest privileges necessary to complete their tasks.
E. LifeX's Product Team shall regularly be reviewing accounts and assigned rights and terminate any of these if not following the above access principles.
F. LifeX shall provide multifactor login for all users of LifeX's proprietary software systems.

## 3.3 User Responsibilities

A. All Users must ensure that their devices are updated and that malware protection is fully functional.
B. All users must lock their screens whenever they leave their desks to reduce the risk of unauthorized access.
C. All users must keep their workplace clear of any sensitive or confidential information when they leave.
D. All users must keep their passwords confidential and not share them.
E. All users shall use multi-factor authentication whenever enabled by the system in use.
F. All users must immediately report to LifeX Incident Response Team (see section 3.7.1) if they have any proof or suspicion that unauthorized access to their own or any colleagues' account has happened or is likely to happen.

## 3.4 Operational reliability and logging

For LifeX's proprietary software systems LifeX shall ensure that;

a. operating procedures are documented and maintained
b. systems that monitors and automatically blocks suspicious activity (including vulnerability scanning, failed logins, and a host of other suspicious activity) are in place
c. information security incidents are registered, risk assessed and reported to relevant parties
d. penetration tests done by third party professionals are run frequently
e. changes in the codebase of the systems are logged and follow a documented change process with relevant approvals and tests.
f. development, test and operational systems are kept separate and that capacity and performance are monitored and managed.
g. security requirements during development are assessed and integrated into the solutions.

## 3.5 Data protection and privacy

A. LifeX shall always comply with relevant national and EU level data protection laws including EU's General Data Protection Regulation (GDPR), whereas the most important principles are:

- ○ Lawfulness, fairness, and transparency: Personal data must be processed in a lawful, fair, and transparent manner, with clear communication to data subjects about how their data is being used.
- ○ Purpose limitation: Personal data should only be collected for specific, explicit, and legitimate purposes, and not further processed in a manner incompatible with those purposes.
- ○ Data minimization: The collection of personal data should be limited to what is necessary for the intended purpose, and no more.
- ○ Accuracy: Personal data must be accurate and, where necessary, kept up to date.
- ○ Storage limitation: Personal data should not be stored for longer than necessary for the intended purpose.
- ○ Integrity and confidentiality: Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing, accidental loss, destruction, or damage.
- ○ Accountability: Data controllers must be able to demonstrate compliance with the GDPR principles, including having appropriate policies and procedures in place.

- See LifeX's general data privacy policy
- See LifeX's general data processing agreement

B. For LifeX's proprietary software systems Customer data resides in shared datastores. We have implemented stringent privacy controls within our application to safeguard data integrity and confidentiality. These measures ensure that one customer's data remains isolated from another's.

### 3.5.1 Encryption

A. All data moving to or from our proprietary systems are encrypted, ensuring it remains confidential and intact.

B. Our API and application endpoints exclusively use TLS/SSL, adhering to the highest standards of data transfer security.

### 3.5.2 Data Location and Use of Sub-Processors

A. LifeX  engages Sub-Processors to assist us with hosting and infrastructure and we may engage with Sub-Processors to support product features and integrations. For LifeX proprietary softwares systems we currently use Render and AWS for our infrastructure and hosting. All data in LifeX proprietary software systems are located in the European Union.
   - See Render's cyber security, data privacy and data protection policies here
   - See AWS' cyber security, data privacy and data protection policies here

B. In general, LifeX shall only use Sub-Processors that are compliant with relevant national and EU level data protection laws including EU's General Data Protection Regulation (GDPR).

## 3.6 Backup

A. LifeX shall always ensure that all data is backed up reliably and that the backups are protected carefully.
B. For LifeX proprietary software systems backups are retained for 7 days and recovery can be made point-in time. This means that data can be restored into a new database at the point in time before data loss occurred up to 7 days.

## 3.7 Incident Response

### 3.7.1 Incident Response Team

A. LifeX's Incident Response Team is responsible for responding to any cyber security incidents, such as data breaches, cyber attacks, and system failure as well as for frequently reviewing and evaluating the incident response plan. The team consist of:

   - LifeX's Chief Executive Officer
   - Team Lead of LifeX's Product Team
   - Team Lead of LifeX's Customer Success Team
   - Key Accounts for Clients of LifeX's proprietary software systems

B. Clients of LIfeX's proprietary software systems shall receive a contact list with contact information on whom to contact in the event of a breach or any other cyber security incident.

C. Clients' appointed Key Account at LifeX will be responsible for communications concerning any data breach or cyber security incident relevant to the specific client as well as during any indecent response process (see below)

### 3.7.2 Incident Response Plan

If an event is raised to the Incident Response Team the team is responsible for the incident response including the following:

1. keeping a detailed log of all activities;
2. initiating incident containment and eradication procedures;
3. activating data loss and recovery process;
4. informing necessary parties, including affected individuals, clients and partners and if necessary, law enforcement, regulatory authorities and media;
5. following data security procedures after the breach is contained, for example, requiring password changes, removal of accounts, or the like;
6. performing analysis to discover how the incident occurred;
7. mitigating any vulnerabilities to prevent future incidents;
8. sending follow-ups, to affected parties;
9. evaluating breach response and improving or amending the response plan.

## 4. Enforcement

Any user found in violation of this policy is subject to disciplinary action that can include terminations of accounts or user access right and, for LifeX employees, termination of employment. Any third-party partner or contractor found in violation may have their network connection terminated.