

Liferay DXP Cloud

Data Security & Protection

Table of Contents

Executive Summary	1
Liferay DXP Cloud: Product Briefing	1
Security is the Foundation of Our Operations	3
Security of Liferay DXP Cloud Services	3
System and Data Security Standards	3
Encryption	4
System Access Control	4
Data Access Control	4
Isolation Control	5
Logging and Integrity	5
Backups	5
Recovery Strategies	5
Availability Commitment	6
Data Retention and Deletion	6
Supplier Management	7
Data Center Locations	7
Security Audits	7
Compliance with Data Protection Laws	7
Moving Forward	8

Executive Summary

It's no secret that the digital world is always changing. As a business in this shifting environment, it is imperative to adapt your digital strategy as technology and security needs change. Customers are looking for fast, easy-to-navigate digital experiences and enterprises need agile, secure environments—meaning the secret to a successful digital strategy lies at the intersection of customer expectations and business value.

All of this leads to businesses operating on the cloud. Empower your organization with technology that supports this digital strategy: Liferay DXP Cloud¹, which pairs an enterprise platform as a service (PaaS) with a powerful digital experience platform. Combined, these solutions act as a powerful and secure platform that can tackle your challenges and help you achieve agile digital transformation.

Liferay DXP Cloud: Product Briefing

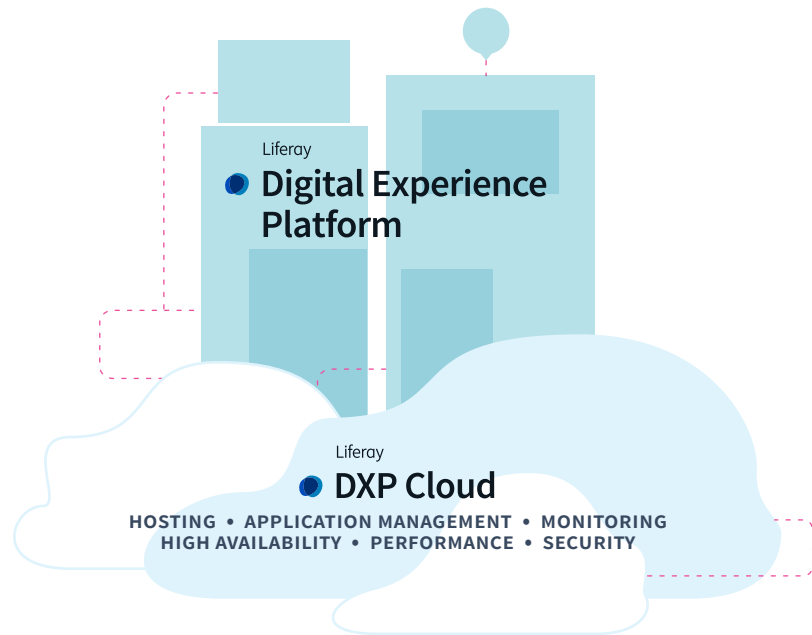
Enable real end-to-end digital transformation with a secure, reliable enterprise PaaS solution that can overcome your business and technical challenges. Designed for Liferay Digital Experience Platform² (DXP), Liferay DXP Cloud speeds time-to-market and improves quality at every stage from infrastructure to web experiences.

Focus on What Matters	Deliver with Confidence	Evolve Faster
Simplify infrastructure management and save IT resources for higher business priorities. Overcome these infrastructure hurdles to more quickly deliver value to your end customers and reduce maintenance costs.	Rest on Liferay's best practices and security enforcements that have been refined over thousands of mission-critical deployments and over 15 years of experience. Liferay DXP Cloud is the best way to deploy Liferay DXP.	Achieve faster time-to-market with enterprise developer tools that boost productivity. Streamline the development cycle with full DevOps features that enable zero downtime deployments.

¹ Liferay DXP Cloud

² Liferay Digital Experience Platform

Liferay DXP Cloud allows your organization to deploy, manage and scale your DXP projects in the cloud, making it easier to quickly overcome the digital challenges faced by business and development teams. Through subscription services, Liferay offers complete packages that include licensing, support, maintenance, legal assurances, exclusive resources created by expert developers and a valuable relationship with the vendor.



Liferay DXP Cloud can help establish a solid groundwork for your business while continually improving and evolving with engaging digital experiences powered by a leading DXP. The enterprise PaaS and DXP work together to enhance each other and enable greater digital transformation.

Security is the Foundation of Our Operations

With more than 250 internal controls and top-notch certifications, such as ISO27001 and SOC2, Liferay DXP Cloud is a robust solution for running your digital experience project with the tools and controls necessary for your IT team — all without worrying about compliance or security.

Our certification program includes:

- SOC 2 Type 1 & 2
- ISO/IEC 27001
- HIPAA
- CSA Corporate Member

Security of Liferay DXP Cloud Services

The Liferay Cloud team approaches the development of products and solutions with a Secure by Design approach. We know that security cannot be taken for granted. Instead, it must be integral to the heartbeat of the underlying technology and architecture. One way we accomplish this is by training our development team. With extensive security awareness courses and the OWASP standard, all Liferay Cloud developers are required to pass the training program before working in the codebase.

Liferay Cloud has also established a rigid Software Development Life Cycle (SDLC), using best practices for code review, testing and QA compliance, as well as deployment strategy. The entire lifecycle is designed to ensure that only clean, secure, tested and reviewed code is released into our production environment.

System and Data Security Standards

Liferay is committed to the safety of customer data. As required by data protection laws such as GDPR and others, Liferay has taken several technical and organizational measures to ensure data security in the cloud. Our operations also come with Liferay's dedicated Security Committee — whose aim is to ensure all the policies, controls and best practices are being followed while driving the improvement and evolution of the security program.

Encryption

Liferay uses strong encryption protocols when customer data is transmitted to Liferay. For all data in transit Liferay uses enforced SSL connections with minimum AES-256 encryption. All data stored in the database is encrypted at rest with 128 bit GCM block ciphers.

System Access Control

Liferay DXP Cloud services are hosted at carefully selected reputable providers that provide hosting servers and infrastructure with industry-leading security standards.

Access to Liferay's office space is physically secured through a badge management system, lockdown procedures and access monitoring.

Additionally, the systems are protected from inappropriate access by employees (team members), but also from unwanted access by non-team members. Therefore all service-related accounts are password protected. Wherever possible, multi-factor authentication (MFA) is enforced for all team members accessing the systems. If MFA is not possible and only basic authentication is available (e.g. computer login), team members are restricted to use only strong passwords.

Account passwords follow strict standards for password strength, including randomly generated or unique from any other account password, at least 12 characters long (ideally, 20-30 characters), not containing any known, personal information like birthdays, cities, or family details, or containing or deriving from any common password words (like "password").

All workstations are protected by a 5-minute automatic locking mechanism along with clean desk policies to ensure private data is not accessible via personal work areas.

Data Access Control

Access control privileges to systems that process data are assigned to users via user roles wherever possible and practical. Roles are established based upon department and job function and are reviewed by Liferay Cloud's Security Committee and updated when the job or departmental functions change.

Liferay personnel are only provided with access to customer information on a need-to-know basis, as required for the performance of specific authorized tasks. Liferay Cloud's Security Committee will revoke any unnecessary access when it does not comply with Liferay Cloud's policy.

All logs and access events are tracked and kept indefinitely. All requests are signed by the request actor in the form of user access token ID.

Isolation Control

Customer databases are segregated in their own virtual machines and every project environment is segregated on its own private network. No production data is used in any development environment.

Logging and Integrity

All server and database history is logged and retained forever. All document creation, changes and deletion are kept in recorded logs. These logs are retained for 6 months and protected against unauthorized tampering by secure redundancy and access controls.

Backups

Redundancies and backups are a key element of Liferay's commitment to secure storage. For the system infrastructure, incremental backup routines are run every 30 minutes and all backups are replicated in different regions, encrypted at rest and permanently retained. For customer data, backup routines for the Database and Documents Library are run by default every day and retained for 30 days.

Recovery Strategies

In the unlikely event of a disaster, Liferay is prepared with recovery strategies at every level. Should a catastrophic incident occur that requires a complete recovery, the entire infrastructure can be brought back online within two hours. Each level of disaster recovery is tested regularly to ensure the safety of customer data. Here's how Liferay's tiers of recovery strategies play out:

1. Platform Level

Liferay DXP Cloud possesses advanced self-healing capabilities to ensure high availability for your applications. Additionally, health checks routinely assess the system's overall health. A fully redundant registry of backups in the platform allows the backup and restore process to run in just a matter of minutes, and if the project has two instances, one will be pulled up to recover data.

2. Server Level: Recovery on Server

If the issue is on the server level, all of the services are automatically relocated to another server in the same availability zone (AZ) and the recovery is completed on the cloud provider's virtual machine (VM). The customer data is not affected because it is already multi-AZ (meaning that it is replicated on more than one server).

3. Availability Zone Level: Recovery on AZ

At this point, the issue is affecting the entire AZ rather than one server. DXP Cloud also has strategies for this, and in the case of such an event, all services are relocated to another server in a different AZ. Again, customer data is not affected because it is already multi-AZ.

4. Region Level: Full Recovery

In the event that a situation affects the entire region, DXP Cloud will start a full-crash recovery process, which takes two hours. Separate disaster recovery environments are supported by DXP Cloud and if utilized, the project would then have a dedicated Disaster Recovery environment for high availability purposes located in another region.

Availability Commitment

Liferay commits to a monthly infrastructure availability (MIA) of 99.95% for a customer's Liferay DXP Cloud project. Designated contacts will receive an email announcement prior to any scheduled downtime and as soon as possible for unplanned downtime. Customers will also have access to the status page which shows downtimes, maintenances and information for all cloud assets and regions.

In the case of planned downtimes, customers can access the reason for the outage and the expected downtime duration from the status page. If there are any further questions during a downtime, our support team will be available to address concerns.

Data Retention and Deletion

Liferay retains customer's data in the Liferay DXP Cloud services for a term of 14 days after expiration of a customer's subscription. During this term, the customer may request and Liferay will provide the customer with access to its data stored in the Liferay DXP Cloud services. Liferay will irretrievably remove all customer data from Liferay DXP Cloud services 30 days after expiration of a customer's subscription.

Supplier Management

Liferay utilizes certain subcontractors, as identified in our Statement on Processing of Customer Data for Cloud Services³, for Liferay DXP Cloud service purposes. All external suppliers involved in the processing of customer data are contractually committed to Liferay to provide at least the same level of security standards as described above. These suppliers are reviewed annually for contractual and policy compliance.

Data Center Locations

Liferay Cloud system hosting is provided by Google Cloud Platform. While the base DXP Cloud platform is hosted in North America, customer applications can be hosted in the location of the customer's choice based on the available locations. Current available hosting locations include North America, South America, Asia and Europe with more locations to come.

Security Audits

Liferay Cloud systems are put under rigorous testing by both internal and external teams. These penetration tests and vulnerability scans are conducted on a regular basis, before every major release and at least once a year.

Compliance with Data Protection Laws

Liferay's commitment to the secure processing of our customer's data in accordance with the applicable data protection laws as described above is documented in Section 11 of the applicable Liferay DXP Cloud Appendix⁴. Customer's data stored in Liferay DXP Cloud subject to GDPR will be processed in accordance with the terms of our Data Processing Agreement referenced in the Liferay DXP Cloud Appendix.

Combine Liferay DXP's flexible architecture and features with your customized solutions for meeting applicable data protection law⁵ requirements to see how Liferay DXP Cloud can accelerate your company's journey to compliance.

³ Statement on Processing of Customer Data for Cloud Services

⁴ Liferay DXP Cloud Appendix

⁵ GDPR Compliance

Moving Forward

When it comes to adapting your digital strategy due to changing security and technology needs, Liferay DXP Cloud is uniquely positioned to help you achieve digital transformation. Build the fast, easy-to-navigate digital environments customers want and the agile, secure environments your business needs on a certifiably reliable and secure platform.

Ready to see Liferay DXP Cloud in action? Request a live customized demo from our Sales team so you can see how DXP Cloud can solve your digital strategy challenges.

[Talk to our Sales team.](#)

[Download the Liferay DXP Cloud Features Overview.](#)



Liferay makes software that helps companies create digital experiences on web, mobile and connected devices. Our platform is open source, which makes it more reliable, innovative and secure. We try to leave a positive mark on the world through business and technology. Hundreds of organizations in financial services, healthcare, government, insurance, retail, manufacturing and multiple other industries use Liferay. Visit us at liferay.com.

© 2020 Liferay, Inc. All rights reserved.