LECTRA

3 REASONS WHY A CLOUD-BASED PLM STRENGHTENS DATA SECURITY

Learn how Lectra cloud application Kubix Link **protects your sensitive information.**

SWIPE ⟶

At Lectra, cloud security is jointly managed by the Lectra cloud operations team and its hosting partner, Microsoft Azure. They work together to ensure that your data will be **stored securely** and **protected against unauthorized access.**

The foundation of our security posture is data security. This means **data encryption, authentication mechanisms, and secure access controls**—the cornerstones of modern cybersecurity—are essential functions of our cloud applications.

01 Data encryption

Cloud service providers employ advanced encryption techniques to safeguard data during both transit and storage. This ensures that sensitive information remains indecipherable to unauthorized entities.

- **The Lectra difference: All data flow is sent through HTTPS. Our databases are encrypted at rest following AES-256 encryption standard.**
- **The benefit to you: Your data is indecipherable to unauthorized parties**

An example from the realm of messaging apps like WhatsApp, where data encryption transforms your messages and media into an unreadable format. This ensures the privacy and security of your conversations. Even if a third party gains access to your messages, they won't be able to decipher the content without the encryption key.

02 Authentication mechanisms

Multi-factor authentication and stringent access controls ensure that only authorized personnel can access critical data and resources, minimizing the risk of breaches.

- **The Lectra Difference: Lectra's administrators for cloud-based solutions use multi-factor authentication to connect to the administration interface.**
- **The benefit to you: Safeguard your digital assets by verifying the identity of users**

A real-world example of the benefits of authentication mechanisms can be seen in online banking systems. These mechanisms, such as username-password combinations, biometric scans, or one-time codes sent to mobile devices, ensure that only authorized users can access their bank accounts.

03

Secure access controls

Cloud-based identity and access management tools provide granular control over user permissions, reducing the risk of insider threats.

- **The Lectra Difference: Microsoft Azure, Lectra’s hosting partner has all the certifications required to assure the proper securities of access and management concerning the physical infrastructure they expose, as a service, to Lectra and ultimately to the Lectra’s customers.**
- **The benefit to you: Limit exposure to malicious actors by dictating who can access what information and under what circumstances**

In the context of a high-security government facility, secure access controls determine which personnel can access specific areas and under what circumstances. This prevents exposure to malicious actors who might attempt unauthorized entry into sensitive locations.

KUBiX LiNK

Conclusion

Our aim is to deliver cloud-based solutions that improve your operational performance and protect your enterprise against unauthorized access, data breaches, and cyber threats. By embracing a cloud-based PLM, fashion organizations can innovate while enjoying scalable, robust, and proactive security measures. **Kubix Link can meet all your PLM and data security requirements.**

LEARN MORE ABOUT KUBIX LINK →