Security & Privacy

The Ex Libris Approach to Security, Privacy, and Reliability

With Ex Libris certified to comprehensive international security and privacy standards, rest assured with reliable and secure cloud-based solutions for higher education.

Information technology is constantly evolving, with advances in areas like big data, deep learning, cloud storage and large-scale processing. Alongside the tremendous benefits this yields, there are some associated security and privacy risks. These can include hostile actors looking for new ways to exploit identity and location data, loss of control over personal information, covert surveillance and manipulation.

In response, data protection regimes and regulations have been crafted to promote multi-layered security, privacy-by-design and proactive risk assessment. Among libraries, this is reflected in the IFLA Code of Ethics, its Privacy in the Library Environment statement, and many similar principles adopted around the world.

At Ex Libris, meeting the rigorous demands of our customers includes adhering to globally recognized security practices, setting effective policies, continuous monitoring, reliable incident response and rapid disaster recovery. Ex Libris maintains a wide spectrum of current cybersecurity, privacy and business continuity certifications.

The most critical data security and system availability features of Ex Libris solutions are transparent, ensuring peace of mind as you maintain, share and develop your collection and services. Read about all these capabilities, as well as the latest data security news and updates, at the Ex Libris Trust Center.

Security:

Protecting Your System is Our Priority

Your institutional data and workflows are highly secured behind layered security controls, strong administrative measures, and up-to-date industry practices.

- Ex Libris secures its cloud-based platform with continuous monitoring and regular multi-tier audits that include tests and assessments of application, network and infrastructure vulnerabilities, as well as third-party patching and security reviews.
- A Chief Information Security Officer and a dedicated cybersecurity team mitigate, investigate and respond to any threats, whether accidental, intentional or malicious.
- Round-the-clock physical security at Ex Libris data centers includes biometrics, intrusion detection systems, interior and exterior surveillance, and authorized access only.
- Ex Libris maintains open and regular communication with you, from sharing policies to issuing vulnerability advisories, patch recommendations and threat alerts.

Security related certifications and compliance

- ISO/IEC 27001:2013 – A standard for security controls used in information security management systems to protect the information of customers and other stakeholders.
- ISO/IEC 27017:2015 – Security controls and implementation guidance for both cloud service providers and cloud service customers.
- ISO/IEC 27032:2012 – Cybersecurity guidance requiring diverse types of controls, including at the application level, to protect servers and end users, and to thwart social engineering attacks.
- SOC 2 Reports for Data Centers– An American Institute of Certified Public Accountants assessment of non-financial reporting controls related to security, availability, processing integrity, confidentiality, and privacy (data center annual report, available upon request).
- FedRAMP Tailored Authorization (for US Government agencies) – The United States government's standardized requirements regarding security assessment, authorization, and continuous monitoring for cloud products and services (Alma, Primo VE, Leganto and Esploro are authorized in the Ex Libris Higher Education Cloud Platform dedicated environment).
- CSA STAR - A publicly available registry of security controls implemented for cloud-based products and services, providing customer visibility and promoting company accountability (self-assessment published on the CSA Star website).

Ex Libris Chief Information Security Officer (CISO)

The Ex Libris CISO develops and implements information security protocols at Ex Libris, and is also the contact point for data protection issues. A Privacy and Regulation Officer and a dedicated security team work alongside the CISO to investigate and resolve breaches, disruptions and vulnerabilities affecting Ex Libris products and services.

- Customer data management issues are handled by the Ex Libris Privacy and Regulation Officer.
- Potential security breaches are addressed by the CISO or the security team.
- System disruptions are escalated to the HUB immediately.

Security and privacy incidents may be reported by an automated diagnostics system, Ex Libris employees, customers, partners or suppliers.

Security concern?
SecurityOfficer@exlibrisgroup.com

Privacy issue?
Privacy@exlibrisgroup.com

Click here to take a virtual tour of one of the Ex Libris cloud services data centers.

Privacy:

Your Data is Under Your Control

As a leader in data privacy in library services, we have implemented a privacy-by-design approach in building all our solutions and cloud-based services.

- Information you provide for using our products or interacting with Ex Libris is processed according to our documented agreements.
- User authorizations can be configured to limit or expand access to information based on the user's role in your organization.
- A Data Protection Officer (DPO) is responsible for monitoring compliance by Ex Libris and its employees with all relevant privacy-related legislation, and seeing that all requests for information are handled promptly and professionally.
- Our SaaS Services allow customers to independently access, update, rectify or erase personal information.

Privacy related certifications and compliance

ISO 27701:2019 – A standard for establishing, implementing, maintaining and continually improving a privacy information management system (PIMS).

ISO/IEC 27018:2014 - A standard for the protection of personally identifiable information in a cloud environment.

GDPR – European Union regulations regarding the collection, handling and processing of personal data.

A Word About GDPR

The GDPR gives individuals greater control over their personal data and imposes many data protection and privacy obligations on organizations in the EU. Ex Libris supports compliance with the GDPR through strong security and privacy frameworks, certified security and privacy controls, and detailed documentation.

- Data Processing Agreement – An addendum incorporating language required by the GDPR into customer agreements for each of our product groups and reflecting data processing activities within Ex Libris services.
- Subprocessor Information – Details regarding affiliates, data center providers and trusted third-party vendors Ex Libris engages as subprocessors to support various solutions and services.
- Privacy Impact Assessments – Reports by a leading privacy consultation firm, regarding data processed in select Ex Libris solutions, the privacy impact, and the measures Ex Libris is taking in order to manage the risks involved.

Reliability:
Your Services Are Available

Reliable, secure and redundant cloud-based architecture provides the integrity and high availability of the Ex Libris applications, services and data on which your organization depends.

- State-of-the-art Ex Libris data centers are designed with physical and environmental security controls, mitigating the impact of single points of failure and ensuring the resilience of the computing center.

- The Ex Libris cloud infrastructure is designed for business continuity and disaster recovery, with full redundancy, load balancing, failover capabilities, redundant firewalls, and more.

- The Ex Libris Network & Security Operations Center (the HUB) provides 24×7, year-round monitoring for all Ex Libris cloud and hosted services, with multi-layered, fully redundant systems to ensure services inside and outside the data center are performing optimally.

- You can always access real-time updates on the status of the Ex Libris cloud services, quarterly reports on system uptime, and root-cause analyses of notable disruptions. Service disruptions can be reported through multiple channels for immediate response.

Reliability related certifications and compliance

- ISO/IEC 22301:2019 – A comprehensive standard for planning, monitoring, maintaining, documenting and continually improving a system for business continuity management and disaster preparedness.

- Compliance with ITIL processes for change management, project management and more.

- Accessibility - A comprehensive VPATs report and statement on compliance with international standards (WCAG) for web content accessibility for people with disabilities.

- Uptime Reports – For SaaS multitenant environments, a quarterly report that measures and tracks system availability.

Click here to learn more about our 24x7 Network & Security Operations Center (the HUB).