

Welcome to the Ex Libris Cloud v2.3

Version 2.3

A newer version is available [here](#)

Introduction

Congratulations! You have joined more than a thousand other costumers of Ex Libris enjoying the benefits of using the Ex Libris Cloud. This document presents the technical details needed to get started and join the Ex Libris Cloud.

Purpose

This document lists the benefits of using the Ex Libris Cloud services together with general instructions for new customers joining the Ex Libris Cloud.

The Cloud Deployment Model

Ex Libris operates a private cloud offering that is available for the sole use of the Ex Libris customer community. This deployment model differs from a public cloud, which is available to the general public or a hybrid cloud, which is a combination of two or more clouds.

Private cloud implementation allows Ex Libris to provide cloud computing-based services without compromising on the architectural control required to provide superior solutions.

Security

Ex Libris is Committed to providing its customers with a secured and reliable environment. Ex Libris has developed a multitiered security model that covers all aspects of cloud-based systems. The security model and controls are based on renowned international protocols and standards, including ISO/IEC 27001:2013, ISO/IEC 27017:2015, ISO/IEC 27018:2014, ISO/IEC 22301:2012, ISO/IEC 27701:2019 and CSA Star Self-Assessment.

Ex Libris has received several security and privacy certifications, including ISO/IEC 27001:2013, ISO/IEC 27017:2015, ISO/IEC 27018:2014, ISO/IEC 22301:2012 and CSA Star Self-Assessment. The ISO/IEC 27018:2014 standard establishes commonly accepted control objectives, including controls and guidelines for protecting Personally Identifiable Information (PII) for the public cloud computing environment in accordance with the privacy principles in ISO/IEC 29100. ISO/IEC 27017:2015 provides a code of practice for information security controls, including guidelines that expand upon the ISO/IEC 27002 standard by adding security controls specifically related to cloud computing. The ISO/IEC 22301:2012 standard focuses exclusively on business continuity management (BCM). The ISO/IEC 27001:2013 standard provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System (ISMS). The ISO/IEC 27701:2019 provides guidance for establishing, implementing, maintaining and continually improving a privacy information management system (PIMS). The CSA Star Self-Assessment provides

transparency and quality assurance for Ex Libris cloud services.

As part of the company's focus on security issues, Ex Libris employs a dedicated Ex Libris Chief Information Security Officer (CISO) who is the contact person for security issues, a Privacy and Regulation Officer for privacy and regulation issues and a dedicated security team that, together with the Cloud Services team, are responsible for the following tasks:

- Applying the security model to all system tiers
- Monitoring and analyzing the infrastructure to detect suspicious activities and potential threats
- Updating the security model and addressing new security threats
- Systematically examining the organization's information security risks, taking into account threats and vulnerabilities
- Designing and implementing a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable
- Issuing periodic security reports to Ex Libris management and customers
- Adopting an overarching management process to ensure that the information security controls continues to meet the organization's evolving information security needs

Ex Libris is committed to securing the information that the customer community stores in our systems. Each one of the controls that form part of our multi-tiered security model is upheld throughout the organization. The security model is constantly monitored and tested to maintain a high level of security, thus granting Ex Libris users—libraries and their patrons—peace of mind with respect to their privacy, confidentiality, integrity, and availability of their data.

For any security related questions or issues, open a support CRM case or contact the Ex Libris Chief Information Security Officer (CISO) at SecurityOfficer@exlibrisgroup.com.

Services You Will Receive

The application is hosted on hardware owned by Ex Libris at a central secured data center. Ex Libris periodically updates and upgrades the system. The following are some key points:

- Hardware maintenance
- 24x7 manned Hub Operation Center
- System Status page
- Monitoring services
- Redundant infrastructure systems – no single point of failure (power, climate control, fire control)
- Redundant infrastructure devices – no single point of failure (routers, switches, firewalls, load-balancers, storage arrays, etc.)
- Robust UPS facilities
- Diesel powered generators (independent power plants)
- No fewer than 3 ISPs providing OC3-level bandwidth to the facility with load balancing
- Backups are stored at the data center and are also saved in a separate offsite secured location

- Hardware and operating system upgrades and patches
- Application upgrades, patches and maintenance
- Security framework based on ISO 27001 certification
- Cloud Security based on ISO 27017 certification
- Privacy based on ISO 27018 certification
- Business continuity management based on ISO 22301 certification
- Privacy information management system (PIMS) based on ISO 27701 certification
- Security control and continuous monitoring
- Application availability based on SLA

Processes and Procedures

Along with the other factors described in this document, Ex Libris adheres to the following practices and procedures to safeguard your systems availability, integrity, and confidentiality:

- **Root Cause Analysis (RCA)** – Ex Libris performs internal root cause analysis for each service interruption for above 5 minutes and takes the necessary steps to avoid them in the future. For SaaS multitenant environments, Ex Libris publishes RCAs in the Customer Knowledge Center
- **Reactive and Proactive Management** – Ex Libris implements reactive and proactive [problem management](#) based on [ITIL](#) in order to minimize both the number and severity of incidents and potential problems.
- **Capacity Management** – The Ex Libris Cloud group oversees capacity planning. Ex Libris products are inherently designed to be highly scalable and following ITIL capacity management processes including multi-layered threshold and alert mechanisms. As part of our capacity planning, our cloud engineers continuously measure & monitor our existing and new implementations, as well as our future growth pipelines, to ensure we always meet capacity requirements. At the same time, our Cloud group monitors our existing customers' growth and the systems' performance trends. This approach ensures that Ex Libris can provision additional hardware and services to meet our growing customers' needs in real time.
- **Change Management** – Ex Libris utilizes change management systems and detailed processes including approval cycles for each change in the cloud. Each change must be approved, recorded, and documented. The system avoids change conflicts and manages activities in the system.
- **Availability** – ([Uptime Quarterly Reports](#)) – For SaaS multitenant environments, Ex Libris has a quarterly availability report that measures and records system uptime services. This report is published and available for customers in the Ex Libris Knowledge Center.
- **Operating Center** – Ex Libris Network & Security Operations Center (NOC/SOC) provides 24x7 logging and monitoring for all logical network access to customer data and information asset usage and is audited. Ex Libris monitoring consists of multi-layered, fully redundant systems that monitor the services inside and outside the Data Center to validate that services are running at the highest performance levels. Reporting methods of service disruption are available at [Ex Libris Service Disruption Policy](#). For more information, see [the 24X7 Hub contact details](#).
- **On-Call Engineers** – Ex Libris has 24x7 on call expert infrastructure engineers such as, Security, Network, DBA, Storage, System, and dedicated On Call Application Developers that are notified by the operating center in the event of a service interruption.

Change Management

In order to prevent an unauthorized change in the cloud environment and maintain the high level of service to our customers, Ex Libris has implemented change management procedures so that all activities are recorded, documented, scheduled, and approved. Every change in cloud production servers must follow the following procedure:

- Planning stage – document and test procedure.
- Approved cycle of procedures - at least 4 eyes approval principle.
- Coordination and notification
- Execution in maintenance time
- Documentation

The Hub 24x7 NOC/SOC and Cloud teams are continuously monitoring and auditing the process.

The Ex Libris Chief Information Security Officer (CISO) validates enforces and audits the procedure, as part of the ISO audit and certification process that all security measures are in place.

Incident Management

In case a security breach has occurred, a customer's data has been compromised or accessed by an unauthorized person, Ex Libris notifies the customer as soon as reasonably practicable (and in any event, within 24 hours), according to the Incident Response Policy.

As part of the Ex Libris security incident response policy, Ex Libris is committed to take prompt action to investigate the incident, mitigate any harm stemming from the incident, and take action intended to prevent any similar incidents from occurring, including, without limitation, the installation of appropriate patches or software fixes as soon as reasonably practical.

After Ex Libris has determined that a security breach has occurred or that customer data has been compromised or accessed by an unauthorized person, Ex Libris shall:

- Notify the customer within 24 hours or sooner if reasonably practical.
- Take prompt action to investigate the incident and mitigate any harm flowing from the incident.
- Assist the customer to make any required notifications to third parties.
- Take prompt action to prevent any similar incident from occurring, including, without limitation, the installation of appropriate patches or software fixes as soon as reasonably possible.

Continuous Monitoring of Security Controls

Ex Libris performs multi-tiered security audits that include:

- Daily security checks
- Monthly security reviews
- Quarterly application security vulnerability assessment scans
- Quarterly third-party patching
- Annual scan of network vulnerabilities

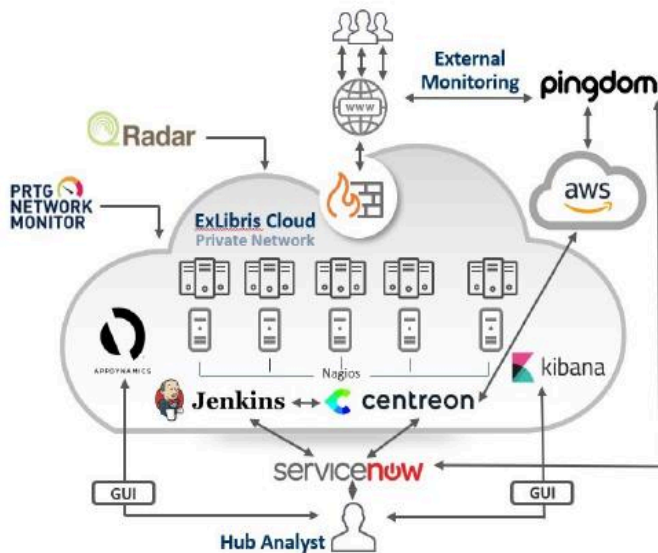
ISO 27001 certification includes annual external audits to validate that all security measures and mitigations are in place.

Additionally, Ex Libris engages an independent security company that performs a security penetration test based on the

Ex Libris Monitoring System

Monitoring cloud operation is at the heart of providing a high level of service. Ex Libris monitoring is built on a multi layered concept.

Monitoring multi-layered conceptual architecture systems include multi-systems that monitor the services inside and outside the Data Center, to validate that services are running with the best performance indicators.



Access Control System

In order to increase monitoring and enforce our access control policies, Ex Libris utilizes an Access Control System, a privileged account security solution that performs the following:

- The access control system is the only focal point through which access to the Ex Libris cloud servers can be made.
- The access control system validates if the user is authorized to access the server.
- The access control system restricts access according to predefined user and policy restrictions.
- Throughout the user's activity on the server, the tool checks and enforces that only approved activity on the server is performed.
- Any session to a production server can only be made through the access control server (i.e., from the authorized Ex Libris employee to the access control system and from the access control system to the server). This way, the access channel itself is controlled.
- All the data related to access rights, credentials, etc. are stored encrypted.
- The predefined sensitive operation activity sessions are recorded and tracked for review.

Ex Libris Security personnel review a correlated audit and compliance report daily. Any suspicious activity, potential violations or unauthorized access is handled immediately according to the Ex Libris Security response policy. These audit and compliance reports contain information that enables Ex Libris to track safe activities in order to meet audit requirements, including privileged accounts compliance status, entitlement reports, and activities logs.

Ex Libris Backup System

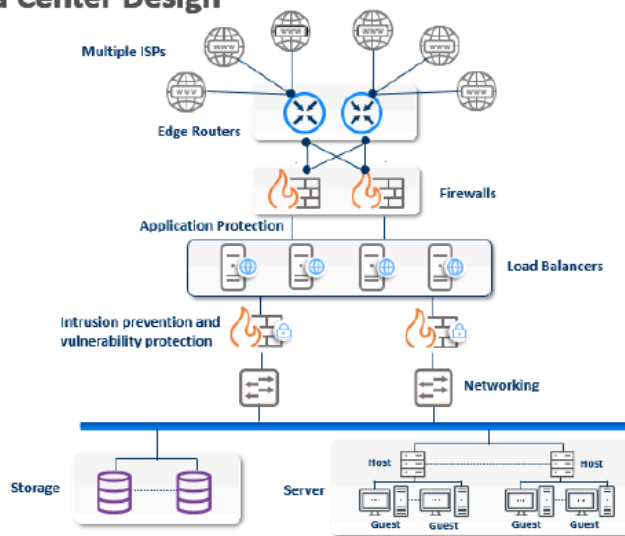
Ex Libris maintains a well-developed backup plan consisting of multiple snapshots per day, including a full daily backup. The backups are made to a disk, a reliable backup media, and are stored in a remote secured location. This ensures that, at any point in time, in case of a local disaster, Ex Libris has a secure copy of the data readily available. On a regular basis, Ex Libris performs system backups of application, database and storage files. The privacy controls in practice at Ex Libris are enforced for all backup files.

- **On-site backup** – Full backups of the OS platform, application, and customer data are performed at least daily (multiple snapshots are taken during the day for critical services/systems) using storage snapshot technology. The backups are kept for one week on-site (not on separate disks) on highly available storage arrays. The snapshots are automatically mounted with specified access restrictions managed by the operating system in a specified set of directories that allows for an easy and immediate restore of the data at any time by Ex Libris authorized personnel.
- **Off-site backup** – Full backups of the OS platform, application and customer data are performed daily using replication technologies over a dedicated and private secured network connection, from the primary data center to an off-site backup location using the same storage technology as at the primary location. Subject to the privacy controls in effect, Ex Libris maintains the off-site backup locations in the same territory (NA, EMEA, and APAC) as the primary locations with a sufficient best practice physical distance. The backups can be restored to the main data center 24x7 by Ex Libris authorized personnel. The backups are kept at the offsite backup managed locations.

The restore procedures are tested monthly to ensure rapid and successful restoration in case of data loss or corruption. Additionally, a full copy of the data is maintained at a remote secured location.

Ex Libris Data Center Network Diagram

Data Center Design



Ex Libris Data Center Network – Security controls at Ex Libris data centers are based on standard technologies and follow international standards. The physical, network, and operational security controls are constructed to eliminate the effect of single points of failure and to retain the resilience of the computing center.

For more information about the location, please visit the [Trust Center](#).

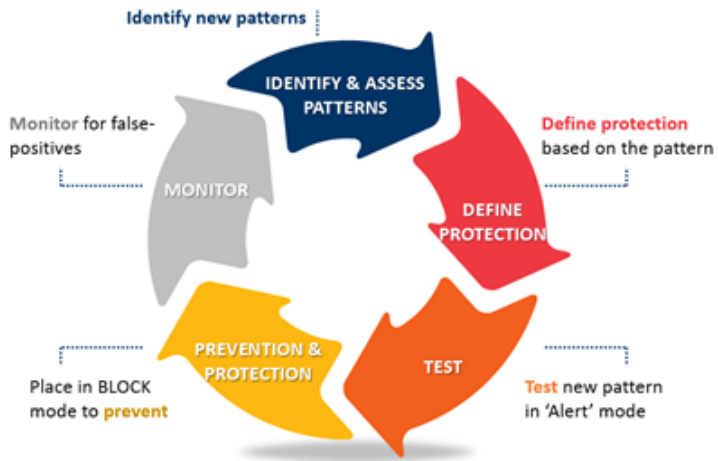
Wireless is not allowed in any Ex Libris data center.

RefWorks and funding solutions (Pivot and Research Professional) are hosted in a public cloud

Ex Libris maintains data centers around the world and has established second data centers in each of the following regions: The United States, Europe, and Asia Pacific, in addition to the existing regional data centers. For more information, see [Ex](#)

Security Layered Protection Approach

Ex Libris implements a layered protection process for ongoing and pro-active protection.



Ex Libris System Status Page

Hosted Customers on SaaS Environments

[The Ex Libris System Status page](#) displays the latest information on the availability of all multitenant Ex Libris instances. You can check this page at any time to see current status information or subscribe to be notified via email of interruptions to any individual service. If you are experiencing a real-time operational issue that is not indicated on this page, please inform Ex Libris by submitting a Case in the Support Portal.

The system status page holds instances for hosted customers on SaaS environments. This site displays live data along with historical data for the previous five days. Customers with single tenant hosted environments can also receive updates on a data center level or on the product within the data center level.

For more details, see: [System Status for Hosted Environments \(Multi-Tenant and Single-Tenant\)](#).

Contact Ex Libris by submitting a Case in the [Support Portal](#).

Single-tenant Hosted Environments

Note: Customers with single-tenant hosted environments can continue to view the status of their services in status.exlibrisgroup.com/single-tenant/






We encourage you to register for these notifications directly from the Support Portal.

When logging into the Support Portal, under your "Email Preferences" tab, you will find the full list of your Ex Libris products. Register here directly to receive updates from Support and the Cloud and automatically subscribe to the System

Status notifications as well.

Performance Indicators

The status of every instance is displayed via a Performance Indicator. More detailed information and timely updates can be found by hovering over these indicators.

Status	Description
 Service is Operating Normally	Service for the instance is operating normally
 Information/Service Alert Information	Service for the instance is operating normally, with some specific information provided by Ex Libris
 Performance Issues	Service for the instance is available, but users may experience performance issues.
 Service Interruption	Service for the instance is unavailable or disrupted
 Scheduled Maintenance	Planned maintenance is taking place

Scheduled Maintenance

Notifications of future scheduled maintenance are published in the Scheduled Maintenance column. Detailed information such as start and end times can be found by hovering over the maintenance dates.

Locating an Instance Name

To locate your hosted instance name on the Support Portal (Salesforce), simply log onto the Support Portal and select the desired account asset. If your environment is on the system status, your instance name will be displayed under the Instance Name on Status Page.

While you can register to the System Status Page notifications directly, we highly encourage you to subscribe to the Email Preferences mailing lists, where you will receive updates from Support and the Cloud and will also automatically be registered to the System Status notifications for your environment.

Other Support Options:

ProQuest. Support

Messages and Alerts

[Link to Salesforce Documentation](#)

[Escalation Policy](#)

[Case Status Definitions](#)

[Contact Us](#)

Welcome, Rael Elstein
- 972EXL Contact

[My Profile](#) | [Logout](#)

Account Asset

Account Asset Detail

Asset Name 972EXL- Alma

Account 972EXL

Status

Subscription- Start Date

Subscription- End Date

Expiration Date

Instance name on Status Page Alma CN01

Cloud Status Notification Subscription

Email notifications regarding performance updates and upcoming maintenance of a hosted instance are sent to the instance’s subscribers.

In the Support Portal, you can set your “Email Preferences”. Setting your email preference for the product will automatically subscribe you to the correct environment in the System Status Page.

If you want to receive email notifications from the Status page only, click the letter icon next to the desired instance and enter a valid email address. An email is sent to activate the subscription. (If you do not receive the email, check your spam box.)

	Instances	Email Alerts	Current Status	Nov-23	N
<input type="checkbox"/>	Alma NA00				
<input type="checkbox"/>	Alma NA01	<input type="text" value="Enter your E-mail"/>			
<input type="checkbox"/>	Alma NA02	<input type="text" value="Enter your institution"/>		<input type="button" value="Subscribe"/>	

Software Updates and Releases for SaaS

Ex Libris Cloud Teams manage and maintain software updates in the cloud applications.

- **Alma, Leganto, Esploro and Primo VE** – Release updates are installed monthly during a maintenance window and

release notes are published to customers.

- **Primo** – Service packs are released on a quarterly basis and installed during a maintenance window, first on a sandbox environment and then on a production environment.
- **RefWorks** – Release updates are installed monthly during a maintenance window and release notes are published to customers.
- **Funding solution (Pivot and research professional)** – Release updates are installed monthly and release notes are published to customers.
- **Summon** – Revision updates are installed monthly and release notes are published to customers.
- **CampusM** – Release updates are installed monthly during a maintenance window and release notes are published to customers.

Note: All SaaS environment scheduled activity is communicated via [The Ex Libris System Status page](#).

Documentation and References

- **Product Features** – Additional information regarding product features can be found in the [Customer Knowledge Center](#) and in the [Trust Center](#).
- **Security and Privacy** – For additional information regarding security and privacy, refer to the [Cloud Security and Privacy Statement](#) in the [Knowledge Center](#) and to the [Trust Center](#).
- **Service Disruption Communication** – Ex Libris maintains a [Service Disruption Communication Policy](#) to ensure that we react appropriately to any actual or suspected events relating to Ex Libris cloud systems and data. This policy defines the steps that Ex Libris personnel must use to provide a process for documentation, appropriate reporting internally and externally, and communication.
- **Questions** – If you have any further questions regarding cloud services, security or any other topics, please log into the [Support Portal \(Salesforce\)](#), and submit a case to our Support staff who will assist you.

Customer Responsibilities

In order to make sure you benefit from Ex Libris cloud services, your local environment needs to be set up correctly to allow for a smooth start with our cloud-based solutions:

- Maintain the connectivity (with acceptable bandwidth) of the workstations and end users to the internet, including network connectivity to the programs and connectivity between the programs and your local applications.
- Work according to the Customer Appropriate Usage Statement (Appendix A: Rules of Behavior).
- Create and maintain firewall settings and open required ports that permit access to the programs.
- In some cases (such as after a MetaLib KB update), technical involvement from the customer may be required.
- In the event of a service interruption, open a system down support CRM case, or contact the [Ex Libris 24x7 Hub](#). For any other issues, open a [support CRM case](#). For more information, see the [Salesforce CRM Customer Portal Documentation](#).

Appendix A: Rules of Behavior

Introduction

Ex Libris provides cloud services for customers using Ex Libris products. Ensuring the security of cloud services is a high priority for Ex Libris. In order to provide secured solutions that help ensure a high level of global security protection of the

cloud infrastructure, Ex Libris requires customer cooperation.

Scope

This policy is intended for Ex Libris customers with access rights to Ex Libris Cloud infrastructures.

Appropriate Usage

The Customer may access the Ex Libris solution and Ex Libris Cloud systems (the "System") on which Customer data is stored within the solution and/or the System for the purpose of utilizing solution functionalities and for configuring solution access rights and privileges in accordance with the solution documentation.

Recommended Security Practices

Ex Libris recommends following the security practices:

- Apply the latest security patches to ensure that vulnerabilities will not compromise the connection to products.
- Wherever possible, use Transport Layer Security (TLS) 1.2 to ensure that your data is encrypted during transmission.
- Adopt industry-standard solutions to secure and protect your authentication credentials, networks, servers and computers.
- Install anti-virus with automatic updates enabled to ensure that the software is always up-to-date.
- Practice "[least privilege](#)" and "[need to know](#)" principles, as defined in Ex Libris Access Control Policy.
- Implement security and privacy awareness and training programs,
- If you have identified a vulnerability, security, or privacy issue, Ex Libris encourages you to identify and report it to Ex Libris in a timely manner, as documented in the Ex Libris [Responsible Disclosure Policy](#).
- Be aware of phishing and malware attempts. In case of suspicious activity, contact the Ex Libris Chief Information Security Officer (CISO).
- Auditing is conducted regularly to detect and provide critical diagnosis of potential or real security issues.

Inappropriate Usage

The Customer is responsible for employing appropriate efforts to prevent unauthorized access to, and use of, Ex Libris solutions and licensor data and must notify Ex Libris as soon as possible of any unauthorized access or use.

Customer and its end users are not permitted to, (i) make available in any way for the use or benefit of any unauthorized party, Ex Libris' solutions, licensor data, related materials, or other proprietary information received from Ex Libris, in whole or in part, unless Ex Libris so consents in writing; (ii) reverse engineer, decompile, or disassemble the solutions or any components thereof except as expressly authorized by law; (iii) violate or abuse the password protections governing access to and use of solutions; (iv) copy, modify, create derivative works from, download, distribute, or store all or any substantial portion of the solutions or licensor data; (v) remove, deface, obscure, or alter Ex Libris' or any third-party's copyright notices, trademarks, or other proprietary rights notices affixed to or provided as part of the solutions, documentation and/or licensor data; (vi) use any robot, spider, scraper, or other automated means to access the solutions or licensor data for any purpose without Ex Libris' written consent; (vii) use or display program logos differing from Ex Libris' own without Ex Libris' prior approval; (viii) store information or materials in the Ex Libris cloud that violates a third party's rights or breaches applicable law; and/or (ix) use the solutions or the licensor data in a way which would violate any applicable laws, rules and regulations.

Customers are not permitted to: (i) perform penetration, vulnerability or security scans or tests or to run any other security

software or action or to run any other automated monitoring on Ex Libris solutions or services; or (ii) attempt to access any program, resource, service or system not included in the customer access rights under the Agreement. In case of shared environments, the customer will access its own data and configurations for management purposes only.

Customers must maintain the confidentiality of any non-public information received from Ex Libris in connection with Ex Libris solutions and/or services, including, but not limited to, product configurations and network diagrams and will not disclose such information or use it for any purpose other than for the customer's own use of the service, as permitted in the Customer's Agreement.

Except with respect to Ex Libris services provided expressly for such purpose (e.g., an identity management service), Customers are not permitted to store user accounts within Ex Libris solutions.

Customers are not permitted to store sensitive personal data, such as government-issued identification numbers, bank, and payment card account information, race, health and medical information, financial records or information concerning sex life or sexual orientation and other similar information, within the Ex Libris solution.

The Customer and its users are not permitted to use an Ex Libris solution to access, store, distribute or transmit any material that:

- is harmful, threatening, defamatory, obscene, harassing or racially or ethnically offensive;
- facilitates illegal activity;
- depicts sexually explicit images or language;
- promotes violence;
- is discriminatory based on race, gender, color, religious belief, sexual orientation, disability, or any other illegal activity;
- causes damage or injury to any person or property;
- consists of malicious code, such as viruses, worms, time bombs, Trojan horses and other harmful or malicious files, scripts, agents or programs; and/or
- violates a third party's rights or breaches applicable law.

Ex Libris reserves the right to disable access to any material or user that breaches the provisions of this policy.

Record of Changes

Type of Information	Document Data
Document Title:	Welcome to the Ex Libris Cloud
Document Owner:	Tomer Shemesh - Ex Libris Chief Information Security Officer (CISO)
Approved by:	Barak Rozenblat - VP Cloud Services
Issued:	Feb 6, 2012

Type of Information	Document Data
Reviewed & Revised:	Sept 23, 2020

Revision Control

Version Number	Nature of Change	Date Approved
1.0	Initial version	Feb 6, 2012
1.1	Review and Update- Tomer S	Feb 13, 2013
1.2	Review and Update- Tomer S	Dec 5, 2014
1.3	Review and Update- Tomer S	Feb 4, 2015
1.4	Review and Update- Tomer S	Apr 12, 2016
1.5	Review and Update- Tomer S	Jul 12, 2017
2.0	Review and Update- Tomer S	Apr 26, 2018
2.1	Review and Update- Tomer S	Jan 3, 2018
2.2	Review and Update- Tomer S	Jun 5, 2019
2.3	Review and Update- Tomer S	Sept 23, 2020

Document Distribution and Review

The document owner will distribute this document to all approvers when it is first created and as changes or updates are made. This document will be reviewed and updated annually or upon written request by an approver or stakeholder. Questions or feedback about this document can be directed to the owner or a listed approver
