Cloud Security and Privacy Statement

Version 2.3

A newer version is available here

Security

This section describes the Ex Libris security procedures.

Introduction

Ex Libris, a ProQuest company, is committed to providing its customers with a highly secure and reliable environment for our hosted and cloud-based applications. We have therefore developed a multi-tiered security model that covers all aspects of hosted and cloud-based Ex Libris systems. The security model and controls are based on international protocols and standards and industry best practices, including ISO/IEC 27001:2013, ISO/IEC 27017:2015, ISO/IEC 27018:2014, ISO 27701, ISO/IEC 22301:2012 and CSA Star Self-Assessment.

Ex Libris has received several security and privacy certifications, including ISO/IEC 27001:2013, ISO/IEC 27018:2014, ISO/IEC 27017:2015, ISO 27701:2019, 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. ISO 27701:2019 specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) as an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organization. The ISO/IEC 22301:2012 standard focuses exclusively on business continuity management (BCM). 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. 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 certification business processes scope are the Development processes, cloud services, global support services, professional services, operational services, library management services, learning & research solutions. The scope service is for all Ex Libris cloud based services.

As part of the company's focus on security issues, Ex Libris employs a Chief Information Security Officer (CISO), a Privacy and Regulation Officer & DPO, and a dedicated Cloud Services team with responsibility for:

- Applying the security model to all system tiers
- Monitoring and analyzing the infrastructure for suspicious activities and potential threats
- Issuing periodic security reports to Ex Libris management and customers
- Dynamically updating the security model and addressing new security threats
- In addition, the Ex Libris Security team is dedicated to:

- 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 the risks that are deemed unacceptable
- Adopting an overarching management process to ensure that the information security controls continue to meet the organization's evolving information security needs

Physical Security Protocols

Security controls at Ex Libris data centers are based on standard technologies and follow the industry's best practices. The physical security controls are constructed in such a way as to eliminate the effect of single points of failure and retain the resilience of the computing center.

SOC2 Reports

The Ex Libris data centers have a Service Organization Control (SOC 2) reports as the result of an in-depth audit of the centers' control objectives and control activities, including controls over information technology and all other related processes.

Environmental Controls

A variety of environmental controls are implemented at the Ex Libris data center facilities.

- Servers are locked inside the infrastructure in a designated area.
- The server area is cooled by a separate air conditioning system, which keeps the climate at the desired temperature to prevent service outage.
- The facilities are protected by a fire suppression system, which protects the computing equipment and has built-in fire, water, and smoke detectors.
- The facilities have on-site generators, which serve as an alternative power source.
- There is 24-hour video surveillance of all entrances and exits, lobbies, and ancillary rooms. The videos are recorded and monitored, and be retained for later use.

Physical Access Control

Physical access to the data center is restricted to personnel with a business need to access the infrastructure. All physical access activities are logged and monitored. All visitors need to be approved beforehand, and the approval is for a limited period of time. Visitors must be accompanied by an authorized employee throughout their visit.

Operational and Information Security Protocols

Operating System

Operating systems used in the cloud are hardened according to best practices in the industry. Only services and components that are necessary to support the application stack are activated; the administrator user always has a password set up, and only necessary ports in the firewall are open.

Network Security

Firewalls: Applications in the hosting and cloud have firewalls installed to shield them from attack and prevent the loss of

valuable customer data. The firewalls are configured to serve as perimeter firewalls to block ports and protocols.

Network-Based Intrusion Detection and Prevention

The combination of an intrusion detection system (IDS) and intrusion prevention system (IPS) installed and tracks all illegal activities. The system sends real-time alerts and proactively blocks communication once a suspicious attack is discovered. The system performs various activities on the network: log collection and analysis from the various machines (firewalls, switches, and routers), file integrity checking, and rootkit detection.

Data Elimination

Ex Libris has strict procedures and a unique policy for handling obsolete data based on the NIST 800-88 standard. These procedures are also applied if a customer decides to stop using our software. Disks and tapes are destroyed once they are no longer needed. Tapes are overwritten with the next use. CDs that are no longer needed are destroyed by a CD/ DVD data crusher or shredder. All storage devices that may need to be used again are cleaned by data wipe software.

Backup

On a regular basis, Ex Libris performs system backups to back up application files, database files, and storage files. All backup files are subject to the privacy controls in practice at Ex Libris. The restore procedures are tested on an ongoing basis to ensure rapid restoration in case of data loss.

Application Security

Development Life Cycle and Maintenance

Ex Libris implements a number of practices to keep each stage of the software development life cycle secure. These include:

- Planning – During the planning stage, the Ex Libris Chief Information Security Officer (CISO) submits a report specifying the product's security requirements. The report includes the security requirements covering all of the solution components, such as the application, the database, and the client side. To manage security issues optimally, the Ex Libris Chief Information Security Officer (CISO) uses various methods, such as access control, auditing, and monitoring.
- Design and Development – The Ex Libris Chief Information Security Officer (CISO) verifies that the design and development of the product are based on our security guidelines. Other security issues are addressed by an additional security-gap requirements document. The security code review is tested on security-sensitive parts of the application.
- Implementation, Testing, and Documentation – Unit, integration, and system testing confirm that security requirements are properly implemented. The requirements are documented and become standard policy.
- Deployment and Maintenance – The Ex Libris Chief Information Security Officer (CISO) is responsible for identifying, managing, and minimizing security vulnerabilities. The Ex Libris Chief Information Security Officer (CISO) also performs quarterly penetration tests or security reviews.

Change Management

In order to prevent an unauthorized change in the cloud environment, and maintain the high level of service to 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, test procedure

- Approved cycle of the procedures, at least 4 eyes approval principle
- Coordination and notifications
- Execution in maintenance time
- Documentation

The Hub 24x7 NOC and Cloud teams are monitor and audit this process. The Ex Libris Security Officer validates the procedure enforced and it is audited as part of the ISO audit and certification process that all security measures are in place.

Access Control

The following items are relevant for access control:

- Access control – Access to the infrastructure is limited, based on role and responsibility and is only available to Operations and Professional Services for maintaining and supporting customers.
- Authentication – Ex Libris also enforces a strict role based password policy that applies to both layers - the operational team members and the application's users. Passwords are stored in an encrypted form, using a one-way encryption method based on an industry-standard hash algorithm. Only the application is able to compare the hashed and entered passwords. In some cases Ex Libris grants the customer full root access and full control. Customers can implement their own password based on their password policy (depending on products, service level, and their contract agreement).
- Authorization and Privacy – Multi-tenancy and shared resources are basic characteristics of the Hosting and SaaS architecture. Resources, such as storage, and networks are shared between users. Data privacy and protection may be compromised, as the European Network and Security Agency explains, if there is “a failure of mechanisms separating storage, memory, routing, and even reputation between different tenants of the shared infrastructure” (http://www.enisa.europa.eu/media/faq...0Computing.pdf). Therefore, strict data isolation is applied in the application to all layers of the application. Data isolation will be defined based on either shared resources using firewall rules for network isolation, Oracle VPD, or separate databases for database isolation and separate files and permissions for files sharing isolation.
  Since the privacy and confidentiality of its customers' data are the company’s top priority, Ex Libris has developed extended authorization controls and additional security processes to protect customer privacy. The authorization mechanism in Ex Libris applications supports the segregation of duties. Segregation of duties is applied in order to minimize the risks and the possibility of misusing privileges.

Ex Libris has instituted the following policies in order to protect customer data:

- Customer data is protected with Oracle technologies.
- Personal information is protected.
- Sensitive personal information such as bank information and credit cards are not stored by Ex Libris.

Customer data, including private data, is deleted based on the Data Elimination section, and backed up customer data is deleted periodically.
All access control activities produce logs with enough information to meet auditing requirements and support usage charges. In addition, access control activities generate notifications to designated users to prevent users from setting up rogue accounts or otherwise modifying access entitlements.

Asset Management

The following items are relevant for asset management:

- Incident Management – NIST defines a computer security incident as “a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.” (http://www.csirt.org/publications/sp800-61.pdf). To handle security incidents effectively, Ex Libris has constructed incident response and notification

procedures.

- Ex Libris employs a dedicated Incident Handling team that responds to security incidents and mitigates risks. The team uses monitoring and tracking tools and performs real-time analysis. Additionally, the team has clear procedures in place for communicating the incidents to any involved party and for handling escalations. Every incident is forwarded to the Ex Libris Chief Information Security Officer (CISO) for assessment and analysis.
- Personnel Security – Ex Libris realizes that the malicious activities of an insider could have an impact on the confidentiality, integrity, and availability of all types of data and has therefore formulated policies and procedures concerning the hiring of IT administrators or others with system access. Ex Libris has also formulated policies and procedures for the ongoing periodic evaluation of IT administrators or others with system access. User permissions are continuously updated and adjusted so that when a user's job no longer involves infrastructure management, the user's console access rights are immediately revoked.
- Background Checks – Once a candidate has been offered a job with Ex Libris and before he or she begins employment, we conduct a background check. For all background checks and reference checks we receive a release from the candidate prior to starting the screening process. We use a third party to conduct our background checks. The standard check includes S.C check, criminal history, employment verification, and reference checks. Any additional checks are conducted based on business needs.

Continuous Monitoring of Security Controls

Ex Libris has implemented multi-tiered security audits on different levels: security checks on a daily basis, security reviews on a monthly basis, application security vulnerability assessment scans on a quarterly basis, as well as third-party patching on a quarterly basis and an annual scan of network vulnerabilities. The ISO 27001 certification that Ex Libris passed successfully includes annual external audits to validate that all security measures and mitigation are in place.

Regulatory Compliance

SOC2 Reports– As described earlier, Ex Libris data facilities went through an in-depth audit of their control objectives and control activities and a SOC2 audit report was issued.

Ex Libris Privacy Policy

Ex Libris privacy policy can be found at http://www.exlibrisgroup.com/category/Privacy.

Record of Changes

Type of Information	Document Data
Document Title:	Cloud Security and Privacy Statement
Document Owner:	Tomer Shemesh - Ex Libris Chief Information Security Officer (CISO)
Approved by:	Barak Rozenblat - VP Cloud Services
Issued:	Apr 18, 2012

Type of Information	Document Data
Reviewed & Revised:	Nov 29, 2020

Revision Control

Version Number	Nature of Change	Date Approved
1.0	Initial version	Apr 18, 2012
1.1	Updated – Tomer S	Apr 22, 2013
1.2	Review and Update- Tomer S	May 20, 2014
1.3	Review and Update- Tomer S	May 1, 2015
1.4	Review and Update- Tomer S	Apr 11, 2016
1.5	Review and Update- Tomer S	Jun 5, 2017
2.0	Review and Update- Tomer S	Apr 26, 2018
2.1	Review and Update- Tomer S	Aug 28, 2018
2.2	Review and Update - Tomer S	Jan 03, 2019
2.3	Review and Update - Tomer S	Nov 29, 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