Cloud Security and Privacy Statement

Version 2.0

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 27018:2014, and CSA Star Self-Assessment.

Ex Libris has received several security and privacy certifications, including ISO/IEC 27001:2013, ISO/IEC 27018:2014, 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. 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).

As part of the company’s focus on security issues, Ex Libris employs a Privacy and Regulation Officer, a Security Officer, 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.

SSAE16 SOC1

The Ex Libris data centers have a SSAE16 SOC1 service auditor's report 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 DoD 5220.22-M 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 security officer 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 security officer uses various methods, such as access control, auditing, and monitoring.
- Design and Development – The security officer 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 security officer is responsible for identifying, managing, and minimizing security vulnerabilities. The security officer also performs quarterly penetration tests or security reviews

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 on page 6, 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.

Regulatory Compliance

SSAE16 SOC1 – As described earlier, Ex Libris data facilities went through an in-depth audit of their control objectives and control activities and a SSAE16 SOC1 audit report was issued.

Ex Libris Privacy Policy

This section describes the Ex Libris privacy policy.

Overview

This privacy policy governs how we use personally identifiable information that we receive and store about individuals such as visitors to the Ex Libris Website, library staff, students, patrons, and other library users (referred to individually as a "User" and collectively as "Users") who use (i) the Website www.exlibrisgroup.com, and other Websites operated by Ex Libris (referred to collectively as the "Website") and/or (ii) Ex Libris products and services that Ex Libris offers ("Products and Services"). We have implemented this privacy policy because user privacy is important to us. We are committed to respecting the Users' privacy and we recognize users' need for appropriate protection and management of any personal information that we receive and store.

Personal Information

Personal Information means any information that may be used to identify a User, including, but not limited to, a User's first and last name, personal profile, home or other physical address, e-mail address or other contact information. It also includes information regarding patron registration, fines, and circulation records. Ex Libris at all times treats such Personal Information as confidential and subject to the terms of this Privacy Policy.

Personal Information Collected and How It is collected

Website

We do not require Website visitors to provide personal information in order to have access to the Website. We may collect personal information that Users choose to provide when filling out registration forms on the Website for different Ex Libris offerings and services, such as events, webinars, or "contact us" requests (collectively, "Contact Us Requests").

Products and Services

We may receive and store personal information about users from our library customers in connection with the products and services that we provide.

The Way We Use Personal Information

We may contact users to respond to their Contact Us Requests, or contact library staff in connection with their use of products and services to which their institutions subscribe. We store personal information only for as long as necessary to respond to Users, to provide the products and services and/or to comply with applicable record retention rules. We will not use personal information to contact patrons of library customers. We will not share, transfer or disclose Users' Personal Information to any third party without each User's express consent, except as expressly stated herein.

Sharing Personal Information

We may share or transfer Personal Information (i) as directed by our library customers, to whom Users originally disclosed their Personal Information; and (ii) as may be required by law. We may also share or transfer Personal Information (i) within the Ex Libris group of companies, but only for the uses described in this Privacy Policy, such as responding to Users; and/or (ii) to third party service providers solely for hosted storage purposes. If we transfer Personal Information to our affiliates, we will do so only if they are first bound by terms at least as restrictive as this Privacy Policy.

User Rights Regarding Personal Information

As required by law, we provide Users with the right to access, correct, or delete any of their Personal Information that we may be holding. Any such request should be forwarded to our Privacy Officer. We may request that Users first attempt to resolve their concern (and show proof thereof) with the library that collected the Personal Information and provided it to us in connection with the Products and Services they access from us.
Any User wishing to exercise his or her privacy rights, to obtain additional information, or to make a comment or complaint regarding this Privacy Policy or its implementation, is invited to contact our Privacy Officer at privacy@exlibrisgroup.com.

Security

The security of Personal Information is important to us. We follow generally accepted industry standards, including the use of appropriate administrative, physical and technical safeguards, to protect the Personal Information submitted to us.

Enforcement/Verification

We conduct compliance audits of our privacy practices to verify adherence to this policy. Where we have knowledge that any of our employees or third-party service providers is using or disclosing personal information in a manner contrary to this policy, we will take reasonable steps to prevent or stop the use or disclosure. We hold our employees and third party providers accountable for maintaining the trust that our Users place in our company.

Personally-Identifiable Information

Personally-Identifiable Information means any information recorded in any form about or concerning an identifiable individual or that can be used, either alone or in combination with other information, to identify an individual, including any information about the goods or services provided by User to such individual. Personally-Identifiable Information shall include information (i) provided by or on behalf of User to Ex Libris; or (ii) obtained, used, accessed, processed, possessed or acquired by Ex Libris on behalf of User or otherwise in connection with the provision of goods and/or services to or for User, including all copies, in whatever form. Personally-Identifiable Information shall be considered Data (as defined below) and shall be safeguarded by Ex Libris in accordance with the terms of this Agreement.

Data

Data means User's information that Ex Libris stores or has stored on behalf of User in connection with the Hosting Services as well as information regarding use of the System by User or the Authorized Users that is generated by the System or by Ex Libris as a result of the Services, including all copies of the foregoing, in whatever form. For the avoidance of doubt, as between Ex Libris and User, User exclusively owns any and all rights in and to all Data. Ex Libris agrees to use or disclose the Data solely for the purpose of providing the Hosting Services. Any Ex Libris employees, contractors or agents ("Representatives") to whom Ex Libris discloses any Data shall be under an obligation (and in the case of non-employees a written obligation) to protect and use the Data in accordance with the terms of this Agreement. Ex Libris shall be responsible for the actions of any of the Representatives to whom it discloses the Data. If Ex Libris becomes aware of any unauthorized access, use or disclosure of the Data or any portion thereof, Ex Libris shall promptly and fully notify User of all facts known to it of such unauthorized use or disclosure

Integrity of the Data

Ex Libris uses commercially reasonable efforts to protect the integrity of the Data. If any Data is lost, destroyed or becomes inaccessible to User, Ex Libris uses its commercially reasonable efforts to recover such Data so it is available for use. If the Data cannot be recovered by Ex Libris within a reasonable period, then Ex Libris will be responsible for paying all reasonable costs and expenses necessary to recreate the Data.

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:	Eyal Alkalay – Ex Libris Sr. Director of Cloud Engineering
Issued:	Apr 18 ,2012
Reviewed & Revised:	Apr 26 ,2018

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

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 approve