Customer Appropriate Usage Statement

Version 2.3

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.

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 services), 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.

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.

Record of Changes

Type of Information	Document Data
Document Title:	Customer Appropriate Usage Statement
Document Owner:	Tomer Shemesh - Ex Libris Chief Information Security Officer (CISO)
Approved by:	Barak Rozenblat – VP Cloud Services
Issued:	Apr 28, 2013
Reviewed & Revised:	July 6, 2022

Revision Control

Version Number	Nature of Change	Date Approved
1.0	Initial version	Apr 28, 2013
1.1	Updated – Tomer S	Apr 24, 2014
1.2	Review and Update- Tomer S	Feb 4, 2015
1.3	Review and Update- Tomer S	Apr 11, 2016
1.4	Review and Update- Tomer S	Mar 22, 2017
2.0	Review and Update- Tomer S	Apr 26, 2018
2.1	Review and Update- Tomer S	Jun 5, 2019
2.2	Review and Update- Tomer S	Apr 25, 2020
2.3	Review and Update- Tomer S	Jun 24, 2021
2.3	Review and Update- Daniel F	July 6, 2022

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