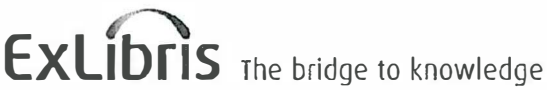
Ex Libris Group
Passwortrichtlinie



VERTRAULICH

Die hierin enthaltenen Informationen stehen im Eigentum von Ex Libris Ltd. bzw. deren verbundenen Unternehmen und jede missbräuchliche Verwendung hat einen wirtschaftlichen Verlust zur Folge. OHNE AUSDRÜCKLICHE SCHRIFTLICHE GENEHMIGUNG VON EX LIBRIS LTD. IST JEGLICHE VERVIELFÄLTIGUNG UNTERSAGT.

Dieses Dokument dient ausschließlich bestimmten Zwecken in Übereinstimmung mit einem bindenden Vertrag mit Ex Libris Ltd. bzw. deren verbundenen Unternehmen. Die hierin enthaltenen Informationen beinhalten Betriebsgeheimnisse und sind vertraulich.

HAFTUNGSAUSSCHLUSS

Die in diesem Dokument enthaltenen Informationen unterliegen regelmäßigen Änderungen und Aktualisierungen. Bitte vergewissern Sie sich, dass Sie über die aktuellste Version des Dokumentes verfügen. Mit diesem Dokument werden weder ausdrücklich noch stillschweigend Gewährleistungen irgendeiner Art abgegeben, mit Ausnahme jener, die ausdrücklich in dem entsprechenden Vertrag von Ex Libris vereinbart wurden. Diese Informationen erfolgen OHNE GEWÄHR. Sofern nicht anderweitig vereinbart, haftet Ex Libris nicht für Schäden aus der Verwendung dieses Dokumentes, einschließlich und ohne Einschränkung Folgeschäden, Bußgelder, indirekter oder direkter Schäden.

Alle Verweise in diesem Dokument auf Materialien Dritter (einschließlich der Webseiten Dritter) erfolgen ausschließlich der Einfachheit halber und stellen in keiner Weise eine Billigung dieser Materialien bzw. Webseiten Dritter dar. Die Materialien Dritter sind nicht Bestandteil der Materialien für dieses Produkt von Ex Libris und Ex Libris haftet nicht für solche Materialien.

Marken

„Ex Libris", The Ex Libris Bridge, Primo, Aleph, Alephino, Voyager, SFX, MetaLib, Verde, DigiTool, Preservation, URM, Voyager, ENCompass, Endeavor eZConnect, WebVoyage, Citation Server, LinkFinder und LinkFinder Plus sowie sonstige Marken sind Marken bzw. eingetragene Marken von Ex Libris Ltd. bzw. deren verbundenen Unternehmen.

Das Fehlen eines Namens bzw. Logos in dieser Liste begründet keinen Verzicht auf die Immaterialgüterrechte von Ex Libris Ltd. bzw. deren verbundenen Unternehmen an ihren Produkten, Features, Servicenamen oder Logos.

In diesem Dokument wird auf die Marken unterschiedlicher Produkte Dritter - wie nachstehend aufgeführt - verwiesen. Ex Libris beansprucht keine Rechte an diesen Marken. Die Verwendung dieser Marken impliziert keine Billigung dieser Produkte Dritter seitens Ex Libris oder die Billigung der Produkte von Ex Libris durch diese Dritte.

Oracle ist eine eingetragene Marke der Oracle Corporation.

UNIX ist eine in den USA und weiteren Ländern eingetragene Marke, ausschließlich lizenziert durch X/Open Company Ltd.

Microsoft, das Microsoft-Logo, MS, MS-DOS, Microsoft PowerPoint, Visual Basic, Visual C++, Win32, Microsoft Windows, das Windows-Logo, Microsoft Notepad, Microsoft Windows Explorer, Microsoft Internet Explorer und Windows NT sind eingetragene Marken und ActiveX ist eine Marke der Microsoft Corporation in den USA und/oder weiteren Ländern.

Unicode und das Unicode-Logo sind eingetragene Marken von Unicode, Inc.

Google ist eine eingetragene Marke von Google, Inc.

Webadresse: http://www.exlibrisgroup.com

Inhalt

Protokollierung von Änderungen

Art der Information	Dokumentdaten
Dokumentname:	Ex Libris Group Passwortrichtlinie
Herausgeber:	Tomer Shemesh – Ex Libris Security Officer
Genehmigt von:	Eyal Alkalay – Ex Libris Cloud Engineering Director
Herausgegeben:	1. März 2011
Geprüft und überarbeitet:	19. April 2015

Verteilung und Prüfung des Dokumentes

Der Herausgeber wird dieses Dokument nach erster Erstellung sowie nach Änderungen bzw. Aktualisierungen an alle Genehmiger verteilen. Dieses Dokument ist jährlich bzw. auf schriftliches Verlangen eines Genehmigers oder Interessenvertreters zu prüfen und zu aktualisieren. Fragen bzw. Feedback zu diesem Dokument können an den Herausgeber bzw. den genannten Genehmiger gerichtet werden.

Überblick

Ex Libris ist verpflichtet, seinen Kunden eine sehr sichere Umgebung für das Hosting und cloudbasierte Anwendungen zu bieten. Daher hat Ex-Libris eine strenge und sichere Passwortrichtlinie und Abläufe entwickelt, die alle IT-Aspekte umfassen, einschließlich Hosting und cloudbasierter Ex Libris-Systeme und -Leistungen.

Passwörter sind ein wichtiger Aspekt der Computersicherheit. Sie bilden die Frontsicherheitslinie für die Benutzerkonten. Ein schwach gewähltes Passwort kann zu einer Gefährdung des gesamten Unternehmensnetzwerkes von Ex Libris führen. Aus diesem Grund müssen alle Mitarbeiter von Ex Libris (einschließlich Vertragspartner und Verkäufer mit Zugang zu den Ex Libris-Systemen) bei der Auswahl und Sicherung ihrer Passwörter geeignete Maßnahmen, wie nachstehend aufgeführt, ergreifen.

Passwörter schützen nicht nur Ex Libris und deren Informationen, sondern auch Sie selbst. Wenn jemand Ihren Account nutzt, können Sie für seine Handlungen zur Verantwortung gezogen werden, wenn Sie dieser Person Ihr Passwort zugänglich gemacht haben.

Zweck

Zweck dieser Richtlinie ist es, einen Standard für die Erstellung sicherer Passwörter zu schaffen, den Schutz und die ordnungsgemäße Verwendung dieser Passwörter zum Schutz von Kundeninformationen sicherzustellen und den Datenschutz durch die Festlegung der Häufigkeit, mit der Passwörter geändert werden sollten, zu wahren.

Geltungsbereich

Diese Richtlinie gilt für alle Mitarbeiter, die über ein Benutzerkonto (bzw. jede Form des Zugangs, die ein Passwort beinhaltet oder erfordert) in irgendeinem System einer Einrichtung von Ex Libris verfügen oder hierfür zuständig sind, Zugang zum Ex Libris-Netzwerk haben, oder nicht öffentliche Informationen von Ex Libris verwahren.

Grundsätze

Allgemeines

Nachstehend sind allgemeine Grundsätze für die Verwendung von Passwörtern aufgeführt:

- Alle Passwörter auf Benutzerebene (wie für E-Mail, Web, Arbeitsplatz, Server-Account usw.) müssen mindestens alle 90 Tage geändert werden. Sofern das Passwort jedoch Bestandteil eines Multifaktor-Authentifizierungsmechanismus (wie z.B. SSH-Schlüssel) ist, ist eine Änderung einmal jährlich akzeptabel.
- Dass Passwort für ein Benutzerkonto mit systemintegrierten Berechtigungen durch Gruppenmitgliedschaften oder Programme wie Sudo, muss sich von dem für alle übrigen Accounts dieses Nutzers verwendeten Passwort unterscheiden.
- Passwörter dürfen nicht in E-Mail-Nachrichten oder sonstigen Formen elektronischer Kommunikation genannt werden. Die Herausgabe von Passwörtern muss mündlich erfolgen.
- Alle Nutzerpasswörter müssen den nachstehenden Richtlinien entsprechen.
- Ein neuer Nutzer ist mit der Option **„Passwort beim nächsten Login ändern"** anzulegen.
- Alle systemintegrierten Passwörter (wie Root, NT Admin, Anwendungsadministrator-Account, Service Account usw.) müssen mindestens alle 6 Monate geändert werden.
- Bei der Neuinstallation eines Ex Libris-Produktes bei einem Kunden ist das Anwendungspasswort zu ändern.
- Bei der Erteilung eines internen Nutzernamens/Passwortes für eine Anwendung an eine externe Quelle (Lieferant, externer Entwickler, Vertriebshändler usw.) muss eine Änderung des Passwortes unmittelbar nach der Session erfolgen.

Richtlinien

Verwende Passwörter müssen sicher sein. Ein sicheres Passwort hat folgende Eigenschaften:

- Komplex:
  - Enthält sowohl Groß- als auch Kleinbuchstaben
  - Enthält Ziffern, Zeichen bzw. Sonderzeichen sowie Buchstaben (z.B. 0-9, (ڎßא(/.,?><';":[]{}` \=-~|+_()*&^%$#@!
- Muss aus mindestens 8 Zeichen bestehen. Systempasswörter müssen aus mindestens 12 Zeichen bestehen
- Erzwungene Passwort-Historie - mindestens 8 Änderungszyklen, bevor ein Passwort wiederverwendet werden kann
- Lockout - Benutzerkonten werden nach 10 aufeinanderfolgenden fehlgeschlagenen Passworteingaben gesperrt
- Muss aus einer nicht trivialen Kombination bestehen.

- Darf kein Wort irgendeiner Sprache, Umgangssprache, eines Dialektes oder eines Jargons bilden
- Darf keinen Bezug zu persönlichen Daten haben
- Darf niemals aufgeschrieben oder unverschlüsselt gespeichert werden
- Versuchen Sie Passwörter zu erstellen, die leicht zu merken sind. Eine Möglichkeit ist es, Passwörter zu erstellen, die auf einem Songtitel, einer Affirmation oder Redewendung basieren. Der Satz könnte zum Beispiel lauten: „This may be one way to remember my password" und das Passwort entsprechend: TmB1w2Rmp! oder Tmb1W>rmp@s.
- Ändern Sie - wenn möglich - den systemintegrierten Nutzernamen.
- Verwenden Sie keine Produktnamen oder Namen, die leicht erraten werden können, wie den systemintegrierten Nutzernamen.

Dagegen ist folgendes charakteristisch für schwache Passwörter und darf daher nicht verwendet werden:

- Das vom System vorgegebene Passwort
- Ein Passwort, bei dem es sich um ein gebräuchliches Wort handelt wie z.B.
  - Namen von Familienmitgliedern, Haustieren, Freunden, Kollegen, fiktionale Charaktere usw.
  - Computerbegriffe, Kommandos, Namen von Firmen, Hardware oder Software
  - Geburtstage und sonstige persönliche Daten wie Anschriften und Telefonnummern
  - Wort- bzw. Zahlenmuster wie aaabbb, qwertz, zyxwvuts, 123321 usw.
  - Alle vorstehenden Passwörter mit einer voranstehenden bzw. nachfolgenden Ziffer
  - Einfache Umwandlungen der vorstehenden Passwörter in Zahlen (1 für l, @ für a, 3 für E usw.)

Passwortschutz

Die folgenden Richtlinien helfen Ihnen dabei, Ihr Passwort zu schützen:

- Teilen Sie Ihr Ex Libris-Nutzerpasswort niemandem mit, einschließlich der Administrations-, Cloud- und IT-Mitarbeiter (es sei denn, Sie ändern es nach Behebung des Problems). Öffnen Sie keinen Fall oder Ticket unter Angabe Ihres Nutzernamens und Passwortes. Bitten Sie stattdessen um Remote-Hilfe und geben Sie das Passwort separat ein. Alle Nutzer- und Systempasswörter sind als sensible, vertrauliche Informationen von Ex Libris zu behandeln. Alle Passwörter sind in verschlüsselten Passwortschutz-Systemen von Ex Libris zu sichern.
- Sofern Cloud-/IT-Mitarbeiter Zugang zu einem System unter Verwendung Ihres Passwortes benötigen, sollten diese Ihr Passwort für die nötigen Arbeiten ändern und es Ihnen nach Abschluss ermöglichen, Ihr Passwort zurückzusetzen.
- Vermeiden Sie die Nutzung der Funktion „Passworterinnerung" in Anwendungen wie PuTTY, SecureCRT, Internet Explorer und anderen Anwendungen.
- Installieren und speichern Sie keine Passwort-Software auf Ex Libris-Computern.

- Schreiben Sie Passwörter nicht auf und verwahren Sie diese nicht in Ihrem Büro oder in der Nähe Ihres Arbeitsplatzes. Speichern Sie Passwörter auf KEINEM Computersystem (einschließlich Mobiltelefone, Tablets oder ähnlicher Geräte) ohne angemessene Verschlüsselung.
- Wenn Sie ein Passwort herausgeben müssen:
  - Tun Sie dies telefonisch und ändern Sie danach das Passwort.
  - Passen Sie auf, wer um Sie herum zuhört.

Sofern der Verdacht besteht, dass ein Account oder Passwort gefährdet ist, melden Sie den Vorfall dem Ex Libris-Sicherheitsbeauftragten und ändern Sie alle Ihre Passwörter in den betroffenen Systemen.

Durchsetzung

Im Rahmen einer halbjährlichen Sicherheitsprüfung durch den Sicherheitsbeauftragten des Unternehmens bzw. dessen Bevollmächtigte kann ein sogenanntes Passwort-Cracking (Knacken des Passwortes) bzw. Passwort-Guessing (Erraten des Passwortes) durchgeführt werden. Das Passwort-Cracking bzw. -Guessing kann auch im Rahmen jährlicher Sicherheitspenetrationstests durch externe Sicherheitsunternehmen und das ISO-Prüfverfahren erfolgen. Sofern bei einer dieser Prüfungen ein Passwort geknackt bzw. erraten wird, so wird dies als Sicherheitsverstoß betrachtet und entsprechend der Sicherheits-Disziplinarrichtlinie verfolgt.