Sicherheitskonzept Alma

in den Bibliotheken der Berliner Universitäten -
Freie Universität Berlin (FU Berlin)
- Humboldt-Universität zu Berlin (HU Berlin)
- Technische Universität Berlin (TU Berlin)
- Universität der Künste Berlin (UdK Berlin)

Erstellt von:
[redacted] (FU Berlin)
[redacted] (TU Berlin)
[redacted] (FU Berlin)
[redacted] (HU Berlin)
[redacted] (UdK Berlin)

Inhalt

Anlagen

Anlage 1: Universitätsspezifische Ergänzungen zum SIKO Alma

(Bibliotheken von FU und HU Berlin: jeweils eine eigene Anlage 1, Bibliotheken von TU und UdK Berlin: eine gemeinsame Anlage 1)

Anlage 2: Ex Libris und Pro Quest

Anlage 3: Rollen und Rechte in Alma

[redacted]

Anlage 5: Notfallrichtlinie von Ex Libris

Anlage 6: Ex Libris Group Passwortrichtlinie

Anlage 7: Notfallplan für die Cloud-Dienste der Ex Libris Group

Anlage 8: Willkommen in der Ex Libris Cloud

I. Darstellung Universität

1. Zielrichtung

Dieses Sicherheitskonzept (SIKO) soll den sicheren Betrieb der Bibliotheksverwaltungssoftware Alma der Firma Ex Libris in den Bibliotheken der Freien Universität Berlin, der Humboldt-Universität Berlin, der Technischen Universität Berlin und der Universität der Künste Berlin gewährleisten. Das SIKO gliedert sich in einen allgemeinen Teil, der für alle Universitäten gleich ist, und in jeweils universitätsspezifische Teile in Anlage 1.

Folgende Ziele sollen gemäß § 5 Abs. 2 BlnDGS mit dem SIKO erreicht werden:

1. Nur Befugte können personenbezogene Daten zur Kenntnis nehmen (**Vertraulichkeit**).
2. Personenbezogene Daten während der Verarbeitung bleiben unversehrt, vollständig und aktuell (**Integrität**).
3. Personenbezogene Daten stehen zeitgerecht zur Verfügung und werden ordnungsgemäß verarbeitet (**Verfügbarkeit**).
4. Personenbezogene Daten können jederzeit ihrem Ursprung zugeordnet werden (**Authentizität**).
5. Es kann festgestellt werden, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (**Revisionsfähigkeit**).
6. Die Verfahrensweisen bei der Verarbeitung personenbezogener Daten werden vollständig, aktuell und in einer Weise dokumentiert, dass sie in zumutbarer Zeit nachvollzogen werden können (**Transparenz**).

Das Konzept und die Risikoanalyse werden auf der Grundlage der Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) zur Sicherheit von CloudSystemen erarbeitet.

- BSI: Dossier Anwender-Management [letzter Zugriff: 06.05.2016]
- BSI (2012): Eckpunktepapier: Sicherheitsempfehlungen für Cloud-Computing-Anbieter – Mindestanforderungen für die Informationssicherheit letzter Zugriff: 06.05.2016]

Das SIKO enthält eine Analyse der Schutzbedürfnisse, eine Bedrohungs- und Risikoanalyse sowie die Darstellung der Sicherheitsmaßnahmen und das Datenschutzkonzept.

Das Bibliotheksverwaltungssystem Alma löst in den vier Bibliotheken das Bibliothekssystem Aleph 500 ab. Mit dem vorliegenden SIKO werden die jeweiligen, für Aleph 500 bestätigten und genehmigten SIKOs abgelöst.

2. Beschreibung des Systems

- Erstellen und Kopieren von Metadaten von gedruckten und elektronischen Büchern und Zeitschriften sowie Datenträgern, Noten und audiovisuellen Medien (im Folgenden Medien)
- Lizenzverwaltung von Medien
- Verwaltung der Kaufinformationen von Medien
- Unterstützung von aktiven und passiven Fernleihen der Bibliothek
- Abbildung der Ausleihprozesse von Medien

Alma bietet über ein Zonen-Konzept an, dass Bibliotheken und verschiedene Arbeitsbereiche kooperieren und Daten untereinander nachnutzen oder austauschen. Die Struktur von Alma umfasst Zonen auf drei Ebenen: die Institutszone, die Gemeinschaftszone und ggf. eine Netzwerkzone:

- **Institutszone (Institutional Zone)** – alle Daten einer Bibliothek

  In der Institutszone werden alle administrativen Daten der Erwerbung und Benutzung der jeweiligen Bibliothek sowie ggf. die bibliographischen Daten gespeichert und von ihren Beschäftigten bearbeitet. Diese Daten sind nur für autorisierte Mitarbeiter_innen der jeweiligen Bibliothek sichtbar und können nur gemäß dem beschriebenen Rollenkonzept (Anlage 3) von diesen Mitarbeiter_innen bearbeitet werden.

- **Gemeinschaftszone (Community Zone)** – Daten, die von ExLibris weltweit für alle Alma-Anwender bereitgestellt werden

  Die Alma Gemeinschaftszone umfasst einen Gemeinschaftskatalog bibliographischer Datensätze, der als Quelle von beschreibenden Datensätzen für alle Alma-Bibliotheken dient und es ihnen ermöglicht, direkt in einem gemeinsamen MetadatenmanagementUmfeld zu arbeiten. Die Bibliotheken können ihren bibliographischen Bestand direkt mit den Gemeinschaftsdatensätzen verlinken oder die Gemeinschaftsdatensätze in den lokalen Katalog kopieren. Bei den Daten in der Gemeinschaftszone handelt es sich um bibliographische Daten, z.B. von E-Medien oder Verlagspublikationen bzw. bibliothekarische Normdaten wie die Gemeinsame Normdatei (GND) der Deutschen Nationalbibliothek.

  Die Gemeinschaftszone wird von der Anwendergemeinschaft gemeinsam verwaltet, Ex Libris beansprucht kein Eigentumsrecht und schränkt die Verwendung oder Wiederverwendung der unter einer offenen Lizenz angebotenen Daten nicht ein.

- **Netzwerkzone (Network Zone)** – Daten, die von kooperierenden Bibliotheken gemeinsam genutzt werden

Für Konsortien oder Verbünde kann in Alma außerdem eine sogenannte Netzwerkzone eingerichtet werden, die bibliographische Titelsätze der an diesem Verbund beteiligten Bibliotheken enthält (vergleichbar mit den heutigen regionalen Verbundkatalogen). Die in einer Institution verwalteten Ressourcen können entweder in der Institutionszone gehalten oder nur mit den bibliographischen Titelsätzen in der Netzwerkzone verlinkt werden, wodurch ein Herunterladen dieser Titelsätze in die Institutionszone überflüssig wird.

Die Mitglieder einer Netzwerkzone können z.B. gemeinsam die dort vorhandenen bibliographischen Daten zur Katalogisierung nutzen. Dieses Modell rationalisiert die Arbeitsabläufe, indem alle Mitglieder die gleichen Oberflächen, Prozesse und Funktionen in einem einheitlichen Arbeitsumfeld nutzen. Das Netzwerk-Konzept sieht aber auch andere Netzwerke vor: für Einkauf, Lizenzierung, Benutzer (gemeinsame Benutzerbasis, Austausch von Benutzerdaten), Ausleihverbund usw.

Die Berliner Alma-Bibliotheken nutzen zurzeit nur die Institutions- und die Gemeinschaftszone. Personenbezogene Daten werden in der Institutionszone gespeichert und verwaltet; die Gemeinschaftszone enthält nur bibliographische Daten. Sollten die Berliner AlmaBibliotheken künftig auch in einer Netzwerkzone arbeiten, wird dies in einem gesonderten Datenschutzverfahren geregelt.

3. Verantwortlichkeiten

Datenverarbeitende Stelle ist die Bibliothek. Die Gesamtverantwortung für das universitäre Bibliothekssystem trägt die Direktorin bzw. der Direktor der Bibliothek.

➢ Weiteres in Anlage 1 – jeweiliger universitätsspezifischer Teil

4. Rechtsgrundlagen des Verfahrens/Einwilligung

2015 haben die Universitätsbibliothek der FU Berlin und die Universität der HU Berlin mit der Firma Ex Libris Deutschland jeweils einen eigenen sowie die Universitäten der TU Berlin und der UdK Berlin einen gemeinsamen EVB-IT Systemvertrag „Vertrag über die Erstellung eines Gesamtsystems" nach deutschem Recht sowie einen „Vertrag zur Datenverarbeitung im Auftrag" (§§ 3,3 a BlnDSG) abgeschlossen, der den Betrieb der Alma-Software auf der Basis „Software as a Service" regelt. Ex Libris Deutschland ist berechtigt, mit Ex Libris Ltd. Israel einen Vertrag als Unterauftragsdatenverarbeiterin in Form eines Auftragswartungsvertrages (BlnDSG § 3) für die Erbringung des Second Level Supports abzuschließen. (Die „Vereinbarung zur Auftragswartung" zwischen Ex Libris Deutschland und Ex Libris Ltd. Israel wurde am 17.02.2015 abgeschlossen entsprechend des vereinbarten Textes in Anlage 7b zum Alma EVB-IT-Vertrag.)

Der EVB-IT Systemvertrag „Vertrag zur Erstellung eines Gesamtsystems", der „Vertrag zur Datenverarbeitung im Auftrag" sowie die „Vereinbarung zur Auftragswartung" wurden in enger Abstimmung mit den behDSB der beteiligten Bibliotheken und dem Berliner DSB formuliert und die Verträge entsprechend des vereinbarten Textes in Anlage 7a-c zum Alma EVB-IT Vertrag geschlossen.

2015 hat die Firma Pro Quest (Ann Arbor, Michigan), ein Anbieter für Content und Recherchelösungen, ein Fusionsabkommen mit Ex Libris Ltd. abgeschlossen. Daraus ergeben sich keine veränderten Verantwortlichkeiten in Bezug auf die mit Ex Libris vereinbarten Datenschutzregelungen (vgl. Anlage 2). Es gelten weiterhin die nationalen datenschutzrechtlichen Regelungen und der Gerichtsstand bleibt unverändert bei einem Vertrag mit Ex Libris Deutschland in Deutschland.

Ex Libris Deutschland ist berechtigt, nach Genehmigung durch den Auftraggeber weitere Unterauftragsdatenverarbeitungsverträge zu schließen, z.B. mit den Betreibern der Rechenzentren in Amsterdam und Zwolle, in denen die Daten der Universitäten und der betriebenen Software gespeichert werden. Diese Verträge beinhalten dieselben Datenschutz- und Sicherheitsvereinbarungen wie im Vertrag zwischen den Universitäten und Ex Libris Deutschland verhandelt.

Die Bibliotheken der Universitäten bleiben als datenverarbeitende Stelle im Sinne des § 4 Abs. 3 Nr. 1 LDSG für die Einhaltung der Vorschriften des LDSG und ggf. anderer Vorschriften über den Datenschutz verantwortlich.

Die Bibliotheken der Universitäten haben das Recht, der Auftragsdatenverarbeiterin (Ex Libris Deutschland) hinsichtlich der Verarbeitung der personenbezogenen Daten Weisungen zu erteilen.

Die Bibliotheken der Universitäten sind berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im Rahmen des Auftragsverhältnisses im erforderlichen Umfang zu kontrollieren oder durch eine von ihnen beauftragte Person kontrollieren zu lassen, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme. Ex Libris unterstützt die Kontrollen.

5. Angaben zu Abhängigkeiten von anderen Systemen / von Alma abhängige Systeme

Das Bibliothekssystem ist abhängig (d.h. Alma bekommt Daten geliefert) von folgenden Systemen:

- *Recherchesystem Primo* o Das Recherchesystem Primo ist die im Internet öffentlich zugängliche Benutzeroberfläche (Front End) für Alma. Primo stellt dafür Funktionen über eine WebSchnittstelle zur Verfügung und kommuniziert mit Alma. Über Primo können die Benutzer_innen ihre Benutzungsdaten in Alma ändern: Vormerkungen und Bestellungen vornehmen, Ausleihfristen verlängern und sich über ihre Leihfristen und Gebühren informieren.

  Bei Nichtverfügbarkeit des Recherchesystems Primo können Benutzer_innen nicht in den Medienbeständen recherchieren und es gibt für sie keinen selbständigen Zugriff auf die Alma-Dienste der Bibliothek. Um die Alma-Dienste zu nutzen, müssen sie sich in die Bibliothek begeben und an das Thekenpersonal wenden.

- *Verbuchungsautomaten / RFID (ID)* o Zum Verbuchen von Ausleihen und Rückgaben eines Mediums in Alma.

  Authentifizierung über Barcode im Studierendendausweis / Bibliotheksausweis bzw. Eingabe von Login/Passwort (bzw. betrifft nur die Bibliothek der HU: Nutzung der HU-Card mit Passwort).

Stehen die Verbuchungsautomaten nicht zur Verfügung, kann die Ausleihe nur an der Theke erfolgen.

- *Fernleihsystem des KOBV* o Die Bibliothek nimmt an der deutschen und internationalen Fernleihe teil.

  Steht das Fernleihsystem nicht zur Verfügung, kann die Bibliothek keine Fernleihbestellungen empfangen und auch keine Fernleihen für ihre Benutzer_innen durchführen.

- *Bibliotheksverbund-Datenbank B3Kat (betrieben vom Bibliotheksverbund Bayern (BVB) mit Sitz in München)*

  o Kooperative Katalogisierung der Bibliotheken Bayerns, Berlins und Brandenburgs o DV-gestützte Anreicherung der bibliographischen Daten durch die Verbundzentrale

  Für die Arbeit der Bibliothek ist die Verfügbarkeit des B3KAT und die Konsistenz der bibliographischen Daten im B3KAT von entscheidender Bedeutung für den korrekten Nachweis der Bestände der Bibliothek. Bei Nichtverfügbarkeit des B3KAT können keine Erwerbungs- und Katalogisierungsarbeiten durchgeführt werden.

➢ Weiteres in Anlage 1 – jeweiliger universitätsspezifischer Teil

Vom Bibliothekssystem sind abhängig (d.h. Alma liefert Daten):

- *Recherchesystem Primo* o Alma verwaltet „im Hintergrund" (Back-End) sämtliche Vorgänge in der Bibliothek, die sich auf die Medien und die Benutzung beziehen.

  Steht Alma nicht zur Verfügung, haben die Benutzer_innen keinen Zugriff auf ihr Bibliothekskonto und können insbesondere keine Vormerkungen oder Verlängerungen vornehmen. Es kann kein Austausch mit dem Recherchesystem Primo erfolgen und der in Primo nachgewiesene Bestand kann nicht aktualisiert werden.

- *Fernleihsystem des KOBV* o Die Bibliothek nimmt an der deutschen und internationalen Fernleihe (gebend und nehmend) teil.

  Steht Alma nicht zur Verfügung, kann die Bibliothek keine Fernleihbestellungen empfangen und auch keine Fernleihen für ihre Benutzer_innen durchführen.

- *Verschiedene bibliographische Datenbanken in Deutschland* o Kooperative Katalogisierung in der Bibliotheksverbund-Datenbank (B3Kat),

  Zeitschriftendatenbank (ZDB), Normdatenbank (GND) o Lieferungen von bibliographischen Daten an Spezialkataloge (Sondersammelgebiete, Fachinformationszentren, regionale Kataloge)

  Die Daten zwischen den abhängigen Katalogen und Alma müssen korrekt sein, da ansonsten ein korrekter Nachweis des Bestands der Bibliothek nicht gewährleistet ist. Darüber hinaus führt es zu zusätzlichem Aufwand, wenn unterschiedliche Bestandsinformationen von verschiedenen Katalogen an Benutzer_innen weitergegeben werden.

- *Mailrelay* o Die Kommunikation von Alma mit der Umgebung erfolgt über Mail. Darüber werden sowohl Mahnungen und Benutzerbenachrichtigungen abgewickelt als auch Listen, Quittungen und alle anderen Schreiben erzeugt.

Fällt das Mailrelay oder das Mailsystem der Universität aus, können keinerlei Schreiben oder Drucke aus Alma erfolgen.

- *IT-Umgebung Einzelplätze* o Nutzung von Alma nach Authentifizierung durch die Mitarbeiter_innen des Bibliothekssystems.

  Fällt Alma aus, sind partiell oder vollständig keine dienstlichen Arbeiten mehr möglich. Ein großes Problem tritt dann auf, wenn davon Ausleihplätze betroffen sind, da keine Ausleihen und Rückbuchungen möglich sind.

➢ Weiteres in Anlage 1 – jeweiliger universitätsspezifischer Teil

5.1 Durch die Bibliothek erhobene und in Alma gespeicherte Daten

	1. Daten	2. Inhalte	3. Erforderlichkeit	4. Datenaustausch/ mit wem	5. Speicherdauer	6. Löschung / Anonymisierung	7. Zugriffsrechte
1	Biblio graphische Daten	Diese Daten werden nach einem jeweils aktuell geltendem Regelwerk (zurzeit RDA) erfasst.	Die Daten dienen einerseits der Information der Benutzer_innen über den Bestand der Bibliothek, andererseits dienen sie dazu, den aktuellen Besitz der Bibliothek (wirtschaftlich) zu belegen. Die Daten sind seit vielen Jahren kontinuierlich erfasst worden. Sie stellen den einzigen Nachweis des Bestandes der Bibliothek dar. Die Korrektheit und Vollständigkeit der Daten ist besonders wichtig.	B3Kat, ZDB, GND, Community Zone	unbegrenzt	keine	autorisierte Mitarbeiter_innen der Bibliothek

2	Etatdaten	Etat-Kürzel, Etat-Bezeichnung, Zugewiesene Mittel, verplante Mittel, verausgabte Mittel	Diese Daten dienen der bibliotheksinternen Verteilung der Erwerbungsmittel, dem internen Nachweis der Verplanung und Verausgabung der Mittel. Die Korrektheit der Daten ist sehr wichtig. Diese Daten spielen keine Rolle in der Kommunikation mit Partnern außerhalb der Universität, da für die Bezahlung von Rechnungen nur die Eingaben in das Haushaltssystem der Universität maßgeblich sind.		unbegrenzt	keine	für den Etat autorisierte Mitarbeiter_innen der Bibliothek

	1. Daten	2. Inhalte	3. Erforderlichkeit	4. Datenaustausch/ mit wem	5. Speicherdauer	6. Löschung / Anonymisierung	7. Zugriffsrechte

3	Lieferantendaten	Ansprechpartner (Name, Vorname, Anrede), Telefonnummern, E-Mail-Adressen, Postalische Adressen, EDIFACT-Adressen, Kontoverbindung, Identifikations-nummern	Die Daten sind für die Abwicklung des Geschäftsverkehrs (Bestellungen, Lieferung, Bezahlung) notwendig. Die unbegrenzte Speicherung ergibt sich aus der Notwendigkeit, bei nicht mehr funktionierenden Dateizugriffen feststellen zu können, wo man den Zugriff gekauft hat. Ggf. wäre zu prüfen, ob eine Löschung 1 Jahr nach Ende der Geschäftsbeziehung möglich ist.		Die Lieferanten der Bibliothek sind in der Regel keine natürlichen, sondern juristische Personen (Buchhandlungen, Agenturen, Verlage usw.), auf die das Datenschutzgesetz nicht zutrifft. Daten natürlicher Personen – sofern Sie mit den juristischen Personen verbunden sind – werden nur in geringem Umfang gespeichert (Ansprechpartner für bestimmte Bereiche, Telefonnummern, E-Mail-Adressen). Hierbei handelt es sich neben Personennamen um rein funktionsbezogene Daten, die auch häufig nicht personalisiert sind (z.B. funktionale E-Mailadressen wie service@degruyter.com ebook@lehmanns.de). Scheiden Ansprechpartner_innen aus Unternehmen aus, werden deren Daten aus dem Lieferantensatz gelöscht oder aktualisiert.	Die Zuordnung von Bestellungen und inventarisierten Beständen zu den Lieferanten als juristischen Personen muss zwingend erhalten bleiben, da dies das zentrale Bestandsverzeichnis der Bibliothek nach LHO darstellt und auch nach Jahren noch regelmäßig Ansprüche/ Fragen mit Lieferanten zu klären sind (Archivrechte, Folgelieferungen usw.). Die Verknüpfung von Bestellung/ inventarisierten Beständen bezieht sich lediglich auf den Lieferantencode, ist jedoch nicht mit personenbezogenen Daten verbunden, die im Lieferantenstammsatz aktuell gepflegt werden.	für die jeweiligen Erwerbungsbereiche autorisierte Mitarbeiter_innen der Bibliothek

	1. Daten	2. Inhalte	3. Erforderlichkeit	4. Datenaustausch/ mit wem	5. Speicherdauer	6. Löschung / Anonymisierung	7. Zugriffsrechte
4	Erwerbungsdaten	Bestellungen, Mahnungen, sonstige Kommunikation zu konkreten Bestellungen mit Lieferanten	Die Daten sind für die Abwicklung des Geschäftsverkehrs (Bestellungen, Lieferung, Bezahlung) notwendig.		Es erfolgt keine Löschung, da ggf. Archivrechte mit diesen Daten verbunden sind.	Es erfolgt keine Löschung, da ggf. Archivrechte mit diesen Daten verbunden sind.	für die jeweiligen Erwerbungsbereiche autorisierte Mitarbeiter_innen der Bibliothek
5	Benutzerdaten	➢ Weiteres in Anlage 1 – jeweiliger universitätsspezifischer Teil					
6	Ausleihdaten	➢ Weiteres in Anlage 1 – jeweiliger universitätsspezifischer Teil					
7	Gebühren	Mahnungen für Medien: Datum, entstandene Gebühren für Dienste und Mahnungen, Mahnungen zu Gebühren, Bezahlung von Gebühren: Ort, Zeitpunkt, Gebührenhöhe, bezahlter Gebührenvorgang	Werden Medien nicht fristgerecht zurückgegeben oder entstandene Gebühren nicht rechtzeitig bezahlt, werden entsprechend der Benutzungs-/ Gebührenordnung gebührenpflichtige Mahnungen ausgesprochen. Diese Vorgänge müssen nachgewiesen und durchgeführt werden.		Gemäß Landeshaushaltsordnung (LHO) Anlage 1 (Nr. 2.10 zu §71) Nr. 2.1: 6 Jahre Beginn der Aufbewahrungszeit gemäß Anlage 1 (Nr. 2.10 zu §71) Nr. 3.1.3: mit Ablauf des Haushaltsjahres, für das sie bestimmt sind	Ende des Haushaltsjahres der letzten Transaktion plus 6 Jahre (s.a. Spalte 5)	alle für die Benutzung autorisierten Mitarbeiter_innen der Bibliothek

8	Kommunikationsdaten	Alle Schreiben, die Alma erzeugt, Ausleih-/ Rückgabe-Quittungen für die Benutzer_innen, Inhalt des Schreibens/ der Quittung, Datum der Erstellung	Alma versendet Schreiben, Quittungen als E-Mails. Diese Schreiben werden im Konto des/r Benutzer_in gespeichert		Schreiben aller Art werden (wg. Einspruchsfrist) 4 Wochen, nachdem der Vorgang abgeschlossen ist, gelöscht.	Löschung in Alma nach der in Spalte 5 angegebenen Frist.	alle für die Benutzung autorisierten Mitarbeiter_innen der Bibliothek

5.2 Maschinell von anderen Systemen nach Alma übermittelte Daten

	Art der Daten	Quellsystem	Inhalte	Erforderlichkeit	Speicherdauer	Rechtliche Grundlage	Datenschutz des Quellsystems	Verantwortlich
1	Bibliographische Daten	B3Kat ZDB GND	Beschreibende Metadaten für alle Medien, die von der Bibliothek erworben oder lizensiert werden	Zur Beschreibung des Besitzes der Bibliothek und zur Information der Benutzer_innen notwendig	unbegrenzt		nicht relevant	nicht relevant
2	Ausleihdaten	Verbuchungsautomaten	Barcode, Name, Vorname, Titeldaten des Mediums, Ausleihe/ Rückgabe	Service der Bibliothek	Während der Ausleihe. Die Ausleihdaten selbst werden danach anonymisiert und für statistische Belange (Ausleihstatistiken) aufgehoben.	Datenschutz-Bestimmungen der jeweiligen Universität	Datenschutz-Bestimmungen der jeweiligen Universität	Leitung der IT der jeweiligen Bibliothek

➢ Weiteres in Anlage 1 – jeweiliger universitätsspezifischer Teil

5.3 Aus Alma maschinell an andere Systeme übermittelte Daten

	Art der Daten	Zielsystem	Inhalte	Erforderlichkeit	Speicherdauer	Rechtliche Grundlage	Datenschutz des Zielsystem	Verantwortlich

1	Bibliographische Daten	B3Kat, ZDB GND Spezialkataloge	Beschreibende Metadaten der Medien, die die Bibliothek besitzt oder lizensiert hat.	Kooperation mit anderen Bibliotheken	unbegrenzt		nicht relevant	nicht relevant
2	Kommu-nikationsdaten	Mailrelay und Mailserver der jeweiligen Universität	E-Mails inkl. Adressen	Kommunikation von Alma für Quittungen, Gebührenbescheide, Erinnerungen usw.	Schreiben aller Art werden (wg. Einspruchsfrist) 4 Wochen, nachdem der Vorgang abgeschlossen ist, gelöscht.	Datenschutz-Bestimmungen der jeweiligen Universität	Datenschutz-Bestimmungen der jeweiligen Universität	Rechenzentrum der jeweiligen Universität

➢ Weiteres in Anlage 1 – jeweiliger universitätsspezifischer Teil

6. Schutzbedarfsfeststellung

Hinsichtlich von

- Vertraulichkeit (keine unbefugte Einsichtnahme)
- Verfügbarkeit (Daten müssen in angemessener Zeit zur Verfügung stehen)
- Integrität (Korrektheit)

Auswirkungen von Verlust von Vertraulichkeit/Verfügbarkeit/Integrität bezüglich

- Beeinträchtigung des informationellen Selbstbestimmungsrechts
- Verstoß gegen Gesetze, Vorschriften, Verträge
- Beeinträchtigung der Aufgabenerfüllung
- negative Außenwirkung der Einrichtung
- finanzielle Auswirkungen

	Daten	Vertraulichkeit	Verfügbarkeit	Integrität	Schutzbedarf (Stufe)

1	Bibliographische Daten	Daten sind frei zugänglich (lesend). Schutzbedarf niedrig	Die Daten sollen 7x24 verfügbar sein. Kurzzeitige Ausfälle sind vertretbar. Ausfälle beeinträchtigen das Ansehen der Einrichtung in geringem Maß. Da die Mitarbeiter_innen nicht handeln können, entsteht hoher materieller Schaden. Schutzbedarf hoch	Die Daten müssen korrekt sein, da sie den Nachweis für den Besitz der Bibliothek darstellen. Die Verletzung der Integrität in einzelnen Daten hat geringe Folgen. Der Verlust der Daten insgesamt ist für den Betrieb der Bibliothek katastrophal. Schutzbedarf hoch	hoch

	Daten	**Vertraulichkeit**	**Ver ügbarkeit**	**Integrität**	**Schutzbedarf (Stufe)**
2	Lieferantendaten	Die Daten sind vertraulich. Die unbefugte Einsichtnahme stellt einen geringen Schaden dar, da diese Daten über andere Informationswege (Internet-Präsenz der Lieferanten selbst) verfügbar sind. Schutzbedarf niedrig	Die Daten müssen zur Arbeitszeit und während der Abarbeitung von Routinejobs (z.B. Erstellung von Schreiben) verfügbar sein. Kurzzeitige Ausfälle sind vertretbar. Ausfälle beeinträchtigen das Ansehen der Einrichtung in geringem Maß. Da die Mitarbeiter_innen nicht handeln können, entsteht hoher materieller Schaden. Schutzbedarf hoch	Die Daten müssen korrekt sein, da Fehler eine Schädigung des Ansehens der Einrichtung darstellen. Schutzbedarf normal	hoch
3	Erwerbungsdaten	Die Daten sind vertraulich. Die Verletzung der Vertraulichkeit kann zu materiellen Schäden (Abbruch von Preisverhandlungen) und Schädigung des Ansehens der Bibliothek führen. Schutzbedarf normal	Die Daten müssen zur Arbeitszeit und während der Abarbeitung von Routinejobs (z.B. Erstellung von Schreiben) verfügbar sein. Kurzzeitige Ausfälle sind vertretbar. Ausfälle beeinträchtigen das Ansehen der Einrichtung in geringem Maß. Da die Mitarbeiter_innen nicht handeln können, entsteht hoher materieller Schaden. Schutzbedarf hoch	Die Daten müssen korrekt sein, da Fehler eine Schädigung des Ansehens der Einrichtung darstellen können. Schutzbedarf normal	hoch

4	Etatdaten	Die Daten sind vertraulich. Die unbefugte Verletzung der Vertraulichkeit kann zu materiellen Schäden (Abbruch von Preisverhandlungen) und Schädigung des Ansehens der Bibliothek führen. Schutzbedarf normal	Die Daten müssen zur Arbeitszeit und während der Abarbeitung von Routinejobs (z.B.: Erstellung von Schreiben) verfügbar sein. Kurzzeitige Ausfälle sind vertretbar. Ausfälle beeinträchtigen das Ansehen der Einrichtung in geringem Maß. Da die Mitarbeiter_innen nicht handeln können, entsteht hoher materieller Schaden. Schutzbedarf hoch	Die Daten müssen korrekt sein. Schutzbedarf hoch	hoch

	Daten	**Vertraulichkeit**	**Verfügbarkeit**	**Integrität**	**Schutzbedarf (Stufe)**
5	Benutzerdaten	Es sind grundsätzlich personenbezogene Daten. Schutzbedarf hoch	Die Daten sollen 7x24 verfügbar sein, damit die Benutzer_innen über Primo auf ihr Konto zugreifen können. Die Daten müssen zur Arbeitszeit und während der Abarbeitung von Routinejobs (z.B.: Erstellung von Schreiben) verfügbar sein. Kurzzeitige Ausfälle sind vertretbar. Ausfälle beeinträchtigen das Ansehen der Einrichtung in geringem Maß. Da die Mitarbeiter_innen nicht handeln können, entsteht hoher materieller Schaden. Schutzbedarf hoch	Die Daten müssen korrekt sein. Schutzbedarf hoch	hoch

6	Ausleihdaten	Es sind grundsätzlich personenbezogene Daten. Schutzbedarf hoch	Die Daten sollen 7x24 verfügbar sein, damit die Benutzer_innen über Primo auf ihr Konto zugreifen können. Die Daten müssen zur Arbeitszeit und während der Abarbeitung von Routinejobs (z.B.: Erstellung von Schreiben) verfügbar sein. Kurzzeitige Ausfälle sind vertretbar. Ausfälle beeinträchtigen das Ansehen der Einrichtung in geringem Maß. Da die Mitarbeiter_innen nicht handeln können, entsteht hoher materieller Schaden. Schutzbedarf hoch	Die Daten müssen korrekt sein. Schutzbedarf hoch	hoch
	Daten	**Vertraulichkeit**	**Verfügbarkeit**	**Integrität**	**Schutzbedarf (Stufe)**
7	Gebührendaten	Es sind grundsätzlich personenbezogene Daten. Schutzbedarf hoch	Die Daten sollen 7x24 verfügbar sein, damit die Benutzer_innen über Primo auf ihr Konto zugreifen können. Die Daten müssen zur Arbeitszeit und während der Abarbeitung von Routinejobs (z.B.: Erstellung von Schreiben) verfügbar sein. Kurzzeitige Ausfälle sind vertretbar. Ausfälle beeinträchtigen das Ansehen der Einrichtung in geringem Maß. Da die Mitarbeiter_innen nicht handeln können, entsteht hoher materieller Schaden. Schutzbedarf hoch	Die Daten müssen korrekt sein. Schutzbedarf hoch	hoch

8	Kommunikationsdaten	Es sind grundsätzlich personenbezogene Daten. Schutzbedarf hoch	Die Daten müssen zur Arbeitszeit und während der Abarbeitung von Routinejobs (z.B.: Erstellung von Schreiben) verfügbar sein. Kurzzeitige Ausfälle sind vertretbar. Ausfälle beeinträchtigen das Ansehen der Einrichtung in geringem Maß. Da die Mitarbeiter_innen nicht handeln können, entsteht hoher materieller Schaden. Schutzbedarf hoch	Die Daten müssen korrekt sein. Schutzbedarf hoch	hoch

7. Risikoanalyse

Zur Risikoanalyse für die in Kap. 6 aufgeführten Daten hinsichtlich Vertraulichkeit, Verfügbarkeit und Integrität wurde das BSI-Eckpunktepapier (s. Kap. 1) herangezogen.

- Die im BSI-Eckpunktepapier geforderten Maßnahmen sind im Alma EVB-IT-Vertrag und seinen 8 Anlagen vertraglich geregelt – erwähnt seien insbesondere die vereinbarten Regelungen zur Sicherheit und zum Umgang mit personenbezogenen Daten in Anlage 7a (Vertrag zur Datenverarbeitung im Auftrag), 7b (Vereinbarung zur Auftragswartung) und 7c (Technische und organisatorische Maßnahmen).
- Die Beschreibung der Sicherheitsmaßnahmen von Ex Libris finden sich im vorliegenden SIKO Alma in Kap. 10 sowie in verschiedenen Dokumentationen von Ex Libris, die dem SIKO als Anlagen beigefügt sind: Anlage 2 (Ex Libris und Pro Quest), [redacted], Anlage 5 (Notfallrichtlinie von Ex Libris), Anlage 6 (Ex Libris Group Passwortrichtlinie), Anlage 7 (Notfallplan für die Cloud-Dienste der Ex Libris Group) und Anlage 8 (Willkommen in der Ex Libris Cloud).

Gesamtergebnis der Risikoanalyse: Aufgrund der vorliegend dokumentierten Sicherheitsmaßnahmen, kommen die Bibliotheken zu dem Ergebnis, dass die Risiken, die sich grundsätzlich aus den Gefährdungen ergeben können, durch die angeführten Sicherheitsmaßnahmen signifikant minimiert sind und Gefährdungsrisiken deshalb nur noch in einem geringen – vertretbaren – Umfang bestehen.

Die Risikoanalyse im Detail:

Gefahrenszenarium und korrespondierende Maßnahmen	Grundbedrohung: Vertraulichkeit Verfügbarkeit Integrität	Grundbedrohung: hohe Vertraulichkeit	Grundbedrohung: hohe Verfügbarkeit	Bedrohte Daten	Sicherheitsmaßnahmen im Einzelnen	Risikobewertung unter Einbeziehung der Sicherheitsmaßnahme
Maßnahmen:						
1 Definiertes Vorgehensmodell für alle IT-Prozesse (z.B. nach ITIL, COBIT)	x			1-8	Ex Libris hat sichere Betriebsabläufe implementiert, basierend auf den ITIL-Best Practices (s. Beschreibung in Kap. 10.1.1; Anlage 8); (s.a. Alma EVB-IT-Vertrag, Anlage 7c).	
2 Implementation eines anerkannten Informationssicherheits-Managementsystems (z. B. durch BSI Standard 100-2 (IT-Grundschutz), ISO 27001)	x			1-8	Ex Libris ist ISO 27001-zertifiziert (s. Beschreibung in Kap. 10.1.1., 10.1.5, 10.2; Anlage 8); (zur ISO 27001Zertifizierung s.a. Alma EVB-IT-Vertrag, Anlage 7c).	
3 Nachhaltige Umsetzung eines Informationssicherheitskonzepts für die Cloud	x			1-8	s. Beschreibung in Kap. 10 sowie die beigefügten Anlagen 4, 5, 6, 7 und 8	
4 Nachweis einer ausreichenden Informations sicherheit (Zertifizierung)		x		5,6,7,8	Ex Libris hat folgende Zertifizierungen: • ISO 27001:2013 (Informationssicherheit) • ISO/IEC 27018:2014 (Personenbezogene Daten) (s. Kap. 10.2)	
			x	1-8		
5 Angemessene Organisationsstruktur für Informationssicherheit beim CSP (Cloud Service Provider) (inklusive Benennung von Ansprechpartnern für Kunden zu Sicherheitsfragen)	x			1-8	Ex Libris beschäftigt einen eigenen Sicherheitsbeauftragten, der u.a. Ansprechpartner für Sicherheitsfragen ist, einen Datenschutzbeauftragten und ein eigenes Sicherheitsteam (s. Beschreibungen in Kap. 10.1.1, 10.1.5, 10.1.7, 10.2; Anlagen 5, 7 und 8)	
B. Rechenzentrumssicherheit Mögliche Gefährdungen ergeben sich z.B.: Elementarschäden, z.B. durch Gewitter oder Hochwasser, oder sonstige Schadensereignisse, z.B. Feuer, Explosion, Unfälle im Straßen-, Schienen-, Wasser- oder Luftverkehr; Naturkatastrophen mit						Das verbleibende Risiko erscheint als so gering, dass das Betriebsrisiko hinsichtlich der genannten Gefährdung als tragbar erscheint.

Gefahrenszenarium und korrespondierende Maßnahmen	Grundbedrohung: Vertraulichkeit Verfügbarkeit Integrität	Grundbedrohung: hohe Vertraulichkeit	Grundbedrohung: hohe Verfügbarkeit	Bedrohte Daten	Sicherheitsmaßnahmen im Einzelnen	Risikobewertung unter Einbeziehung der Sicherheitsmaßnahme
A. Sicherheitsmanagement beim Anbieter Mögliche Gefährdungen betreffen z.B.: Störungen oder Ausfälle von Ressourcen (z.B, Virtualisierungsserver, virtuelle Maschine, LoadBalancer, etc.), insbesondere wenn sie nicht zeitnah erkannt werden						Das verbleibende Risiko erscheint als so gering, dass das Betriebsrisiko hinsichtlich der genannten Gefährdung als tragbar erscheint.

n

Gefahrenszenarium und korrespondierende Maßnahmen	Grundbedrohung: Vertraulichkeit Verfügbarkeit Integrität	Grundbedrohung: hohe Vertraulichkeit	Grundbedrohung: hohe Verfügbarkeit	Bedrohte Daten	Sicherheitsmaßnahmen im Einzelnen	Risikobewertung unter Einbeziehung der Sicherheitsmaßnahme
begrenzter Breitenwirkung wie Flusshochwasser; Eindringen unbefugter Personen						
Maßnahmen:						
6 Redundante Auslegung aller wichtigen Versorgungskomponenten (Strom, Klimatisierung der RZ, Internetanbindung, Verkabelung, etc.)	x			1-8	Ex Libris nutzt ein Colocation-Rechenzentrum, das SSAE-16-sicherheitszertifiziert ist (s. Beschreibung in Kap. 10.1.2 sowie Anlage 7); (s.a. Alma EVB-IT-Vertrag, Anlage 7c).	
7 Überwachung des Zutritts: Zutrittskontrollsystem, Videoüberwachungssysteme, Bewegungssensoren, Sicherheitspersonal, Alarmsysteme, etc.	x			1-8	Die Rechenzentren haben eine umfassende Zutrittskontrolle (s. Beschreibung in Kap. 10.1.2 und 10.1.7; Anlagen 4 und 7); (s.a. Alma EVB-IT-Vertrag, Anl. 7c).	
8 Zwei-Faktor-Authentisierung für den Zutritt ins Rechenzentrum	x			1-8	s.o. # 7	
9 Brandschutz: Brandmeldeanlage, Brandfrüherkennung, geeignete Löschtechnik, regelmäßige Brandschutzübungen	x			1-8	s.o. # 6	
10 Robuste Infrastruktur, die ausreichenden Widerstand gegen Elementarschäden und unbefugtes Eindringen bietet	x			1-8	s.o. # 6	
11 Redundante Rechenzentren, die mindestens so weit voneinander entfernt sind, dass ein beherrschbares Schadensereignis nicht gleichzeitig das ursprünglich genutzte Rechenzentrum und das, in dem die Ausweichkapazitäten genutzt werden, beeinträchtigen			x	1-8	Die beiden Rechenzentren von Ex Libris in Amsterdam und Zwolle liegen mehr als 100 Kilometer voneinander entfernt (s. Beschreibung in Kap. 10.1.2; Anlage 7); (s.a. Alma EVB-IT-Vertrag, Anlage 7c).	

Gefahrenszenarium und korrespondierende Maßnahmen	Grundbedrohung: Vertraulichkeit Verfügbarkeit Integrität	hohe Vertraulichkeit	hohe Verfügbarkeit	Bedrohte Daten	Sicherheitsmaßnahmen im Einzelnen	Risikobewertung unter Einbeziehung der Sicherheitsmaßnahme
C. Server-Sicherheit Mögliche Gefährdungen ergeben sich z.B. durch: Angriffe wie Rechteüberschreitungen von Nutzern, Login-Fehlversuche oder Schadsoftware (z.B. Trojanische Pferde)						Das verbleibende Risiko erscheint als so gering, dass das Betriebsrisiko hinsichtlich der genannten Gefährdung als tragbar erscheint.
Maßnahmen:						
12 Technische Maßnahmen zum Schutz des Hosts (Host Firewalls, regelmäßige Integritätsüberprüfungen, Host-based Intrusion Detection Systems)	x			1-8	Ex Libris hat zahlreiche Sicherheitsmaßnahmen zum Schutz der Hosts implementiert (s. Beschreibungen in Kap. 10.1.3, 10.1.4 und 10.1.5; Anlage 7); (s.a. Alma EVB-IT-Vertrag, Anlage 7c).	
13 Sichere Grund-Konfiguration des Hosts (z.B. Einsatz gehärteter Betriebssysteme, Deaktivierung unnötiger Dienste, etc.)	x			1-8	Ex Libris hat sichere Host-Verfahren als Teil der Bereitstellung für Installation neuer Server und Dienste implementiert (s. Beschreibung in Kap. 10.1.3 und 10.1.4; Anlage 7); (s.a. Alma EVB-IT-Vertrag, Anl. 7c).	
14 Einsatz zertifizierter Hypervisoren (Common Criteria mindestens EAL 4)		x		5,6,7,8	Die eingesetzten Hypervisoren durchlaufen vor ihrer Implementierung ein Verfahren inkl. Änderungsmanagement und Qualitätsanalyse. Ex Libris nutzt die Red Hat KVM (Kernel-based Virtual Machine) Community Edition, die eine EAL 4+ Zertifizierung besitzt.	
			x	1-8		
D. Netzsicherheit Mögliche Gefährdungen ergeben sich z.B. durch: Ablage von Schadprogrammen und „Kapern" der Rechner, um z.B. die Rechner für Spam-versand oder deren Rechenleistung für Brute-Force-Angriffe						Das verbleibende Risiko erscheint als so gering, dass das Betriebsrisiko hinsichtlich der genannten Gefährdung als

n

Gefahrenszenarium und korrespondierende Maßnahmen	Grundbedrohung: Vertraulichkeit / Verfügbarkeit / Integrität	Grundbedrohung: hohe Vertraulichkeit	Grundbedrohung: hohe Verfügbarkeit	Bedrohte Daten	Sicherheitsmaßnahmen im Einzelnen	Risikobewertung unter Einbeziehung der Sicherheitsmaßnahme
zu nutzen; Distributed Denial of Service-Angriffe (DDoS-Angriffe), sowohl externe als auch interne durch andere Cloud-Kunden; Sicherheitslücken, Fehlfunktionen und/oder Ausfälle durch Fehlkonfiguration des Systems						tragbar erscheint.
Maßnahmen:						
15 Sicherheitsmaßnahmen gegen Malware (Virenschutz, Trojaner-Detektion, Spam-Schutz, etc.)	x			1-8	Ex Libris hat zahlreiche Sicherheitsmaßnahmen zum Schutz vor böswilligem Zugriff aus dem Internet implementiert (s. Beschreibung in Kap. 10.1.1 und 10.1.5, Anlagen 4 und 7); (s.a. Alma EVB-IT-Vertrag, Anlage 7c).	
16 Sicherheitsmaßnahmen gegen netzbasierte Angriffe (IPS/IDS-Systeme, Firewall, Application Layer Gateway etc.)		x		5,6,7,8	s.o. # 15	
			x	1-8		
17 DDoS-Mitigation (Abwehr von DDoS-Angriffen)			x	1-8	s.o. # 15	
18 Geeignete Netzsegmentierung (Isolierung des Management-Netzes vom Datennetz)	x			1-8	Die Datenisolation erfolgt auf der Grundlage von Gruppenlaufwerken, separaten Datenbanken für eine Datenbankisolation oder separaten Dateien und Berechtigungen für eine Filesharing-Isolation (s. Beschreibung in Kap. 10.1.6); (s.a. Alma EVB-ITVertrag, Anlage 7c).	
19 Sichere Konfiguration aller Komponenten der Cloud-Architektur	x			1-8	Alle Komponenten basieren auf einem festgelegten Sicherheitsstandard und durchlaufen vor ihrem Einsatz in der Produktion Tests und Kontrollverfahren sowie eine Qualitätsanalyse (s.a. Beschreibungen in Kap. 10.1.3, 10.1.4 und 10.1.5); (s.a. Alma EVB-IT-Vertrag, Anlage 7c).	

n

Gefahrenszenarium und korrespondierende Maßnahmen	Grundbedrohung: Vertraulichkeit Verfügbarkeit Integrität	Grundbedrohung: hohe Vertraulichkeit	Grundbedrohung: hohe Verfügbarkeit	Bedrohte Daten	Sicherheitsmaßnahmen im Einzelnen	Risikobewertung unter Einbeziehung der Sicherheitsmaßnahme
20 Fernadministration über einen sicheren Kommunikationskanal (z. B. SSH, IPSec, TLS/SSL, VPN)	x			1-8	Die Fernwartung und die gesamte Kommunikation erfolgt über verschlüsselte Verbindungskanäle (s. Beschreibung in Kap. 10.4); (s.a. Alma EVB-IT-Vertrag, Anlage 7c).	
21 Verschlüsselte Kommunikation zwischen CloudComputing Anbietern und Cloud-Computing Nutzer (z. B. TLS/SSL)	x			1-8	s.o. # 20	
22 Verschlüsselte Kommunikation zwischen Cloud Computing-Standorten	x			1-8	s.o. # 20	
23 Verschlüsselte Kommunikation mit Drittdienstleistern, falls diese für das eigene Angebot notwendig sind	x			1-8	s.o. # 20	
24 Redundante Vernetzung der Cloud-Rechenzentren			x	1-8	Ex Libris verfügt über umfangreiche Präventivmaßnahmen und Redundanzstrategien ein (s. Anlage 7).	
E. Anwendungs- und Plattformsicherheit Mögliche Gefährdungen ergeben sich z.B. durch: Angriffe auf Applikationsebene durch Sicherheitslücken aufgrund von Programmierfehlern (z.B. Endlosschleifen oder Null-Pointer-Exceptions) oder aufgrund des Einsatzes nicht ordnungsgemäß getesteter Programme bzw. Module						Das verbleibende Risiko erscheint als so gering, dass das Betriebsrisiko hinsichtlich der genannten Gefährdung als tragbar erscheint.
Maßnahmen:						
25 Sicherheit muss Bestandteil des Software Development Life Cycle-Prozesses sein (Reviews, Automatisierte Tests, Vulnerability Tests, etc.)	x			1-8	Sichere Verfahren sind Bestandteil des System Development Life Cycle von Ex Libris (s. Beschreibung in Kap. 10.1.5); (s.a. Alma EVB-IT-Vertrag, Anlage 7c).	

n

Gefahrenszenarium und korrespondierende Maßnahmen	Grundbedrohung: Vertraulichkeit Verfügbarkeit Integrität	Grundbedrohung: hohe Vertraulichkeit	Grundbedrohung: hohe Verfügbarkeit	Bedrohte Daten	Sicherheitsmaßnahmen im Einzelnen	Risikobewertung unter Einbeziehung der Sicherheitsmaßnahme
26 Einhaltung von Sicherheits-Mindeststandards der zur Verfügung gestellten Webanwendungen (z.B. Prinzipien zur sicheren Software-Entwicklung gemäß OWASP - Open Web Application Security Project)	x			1-8	Die Anwendungen von Ex Libris erfüllen mindestens OWASP Top 10 (s. Beschreibung in Kap. 10.1.5); (s.a. Alma EVB-IT-Vertrag, Anlage 7c).	
27 Patch- und Änderungsmanagement (zügiges Einspielen von Patches, Updates, Service Packs) sowie Release Management	x			1-8	Ex Libris hat entsprechende Verfahren im Einsatz (s. Beschreibung in Kap. 10.1.4; Anlagen 7 und 8); (s.a. Alma EVB-IT-Vertrag, Anlage 7c).	
28 Sicherstellung der Patchverträglichkeit auf Testsystemen vor Einspielen in Wirkbetrieb.	x			1-8	s.o. # 27	
F. Datensicherheit Mögliche Gefährdungen ergeben sich z.B. durch: Unerlaubte Datenzugriffe über eine SQL-Injection durch andere SaaS-Kunden; Datenverlust, z.B. durch unzureichende Sicherung oder die Unmöglichkeit, Daten aus dem Backup zu rekonstruieren; unvollständige Löschung der Daten nach Vertragsende						Das verbleibende Risiko erscheint als so gering, dass das Betriebsrisiko hinsichtlich der genannten Gefährdung als tragbar erscheint.
Maßnahmen:						
29 Datensicherheit im Lebenszyklus der Kundendaten definieren und umsetzen	x			1-8	Ex Libris-Kunden behalten die vollständige Kontrolle über ihre Daten (s. Beschreibung in Kap. 10.1.5); (s.a. Alma EVB-IT-Vertrag, Anlage 7c).	
30 Sichere Isolierung der Kundendaten (z.B. virtuelle Speicherbereiche, Tagging, etc.)	x			1-8	s.o. # 18	

Gefahrenszenarium und korrespondierende Maßnahmen	Grundbedrohung: Vertraulichkeit Verfügbarkeit Integrität	hohe Vertraulichkeit	hohe Verfügbarkeit	Bedrohte Daten	Sicherheitsmaßnahmen im Einzelnen	Risikobewertung unter Einbeziehung der Sicherheitsmaßnahme
31 Regelmäßige Datensicherungen, deren Rahmenbedingungen (Umfang, Speicher-intervalle, Speicherzeitpunkte und Speicher-dauer) für die Kunden nachvollziehbar sind	x			1-8	Ex Libris führt regelmäßige Backups an seinen zwei Standorten durch, gemäß seiner Backup-Strategien (s. Beschreibung in Kap. 10.5; Anlagen 7 und 8); (s.a. Alma EVB-IT-Vertrag, Anlage 7c).	
32 Daten müssen auf Wunsch des Kunden vollständig und zuverlässig gelöscht werden	x			1-8	Die vollständige Löschung ist vertraglich vereinbart (s. Beschreibung in Kap. 10.1.5); (s.a. Alma EVB-ITVertrag, Anlage 7c).	
G. Schlüsselmanagement Mögliche Gefährdungen ergeben sich z.B. durch: Verletzung der Vertraulichkeit, Integrität oder Authentizität der Schlüssel						Das verbleibende Risiko erscheint als so gering, dass das Betriebsrisiko hinsichtlich der genannten Gefährdung als tragbar erscheint.
Maßnahmen:						
33 Best Practices der Schlüsselverwaltung umsetzen	x			1-8	Ex Libris verwendet ausschließlich zugelassene Verschlüsselungsverfahren unter Verwendung von Best Practices (s. Beschreibung in Kap. 10.4; Anlage 7); (s.a. Alma EVB-IT-Vertrag, Anlagen 7a und 7c).	
34 Krypto-Übersicht für Kunden zugänglich machen		x		5,6,7,8	Öffentliche SSL-Zertifikate sind verfügbar (s. Kap. 10.4)	
H. ID- und Rechtemanagement Mögliche Gefährdungen ergeben sich z.B. durch: Zugriff auf die IT-Ressourcen durch unbefugte Personen; Einsichtnahme in Daten durch unbefugte Personen						Das verbleibende Risiko erscheint als so gering, dass das Betriebsrisiko hinsichtlich der genannten Gefährdung als tragbar erscheint.

n

Gefahrenszenarium und korrespondierende Maßnahmen	Grundbedrohung: Vertraulichkeit Verfügbarkeit Integrität	hohe Vertraulichkeit	hohe Verfügbarkeit	Bedrohte Daten	Sicherheitsmaßnahmen im Einzelnen	Risikobewertung unter Einbeziehung der Sicherheitsmaßnahme
Maßnahmen:						
35 Starke Authentisierung (Zwei-Faktor-Authentisierung) für Administratoren des CSP (Cloud Service Provider)	x			1-8	Ex Libris setzt umfangreiche End-to-End-Kontrollmechanismen für alle Aktivitäten in der Cloud-Umgebung ein, u.a. starke Authentifizierungsverfahren ein (s. Beschreibung in Kap. 10.1.2 und 10.1.7; Anlagen 4 und 7); (s.a. Alma EVB-IT-Vertrag, Anlage 7c).	
36 Rollenbasierte Zugriffskontrolle und regelmäßige Überprüfung der Rollen und Rechte	x			1-8	s.o. # 35	
37 Least Privilege Model (Nutzer oder CSP-Administratoren sollen nur die Rechte besitzen, die sie zur Erfüllung ihrer Aufgabe benötigen)	x			1-8	s.o. # 35	
38 Vier-Augen-Prinzip für kritische Administrationstätigkeiten		x		5,6,7,8	s.o. # 35	
			x	1-8		
39 Starke Authentisierung (z.B. Zwei-FaktorAuthentisierung) für Cloud-Kunden		x		5,6,7,8	Die Authentifizierungs-Infrastruktur vpm Alma nutzt Identitätsprovidersysteme unter Verwendung von Standardprotokollen wie LDAP und SAML2 (s. Beschreibung in Kap. 10.1.7)	
I. Kontrollmöglichkeiten für Nutzer Mögliche Gefährdungen ergeben sich z.B. durch: Verletzung des SLA, z.B. bei der Verfügbarkeit der Services						Das verbleibende Risiko erscheint als so gering, dass das Betriebsrisiko hinsichtlich der genannten Gefährdung als tragbar erscheint.

Gefahrenszenarium und korrespondierende Maßnahmen	Grundbedrohung: Vertraulichkeit Verfügbarkeit Integrität	hohe Vertraulichkeit	hohe Verfügbarkeit	Bedrohte Daten	Sicherheitsmaßnahmen im Einzelnen	Risikobewertung unter Einbeziehung der Sicherheitsmaßnahme
Maßnahmen:						
40 Kunden müssen die Möglichkeit haben, messbare Größen, wie im SLA vereinbart, zu überwachen	x			1-8	Die Kunden erhalten Cloud-Statusbenachrichtigungen per E-Mail und können die Systemstatusseite mit Informationen über die Verfügbarkeit aufrufen (s. Anlage 8); (s.a. Alma EVB-IT-Vertrag, Anlage 3).	
J. Monitoring und Security Incident Management Mögliche Gefährdungen ergeben sich z.B. durch: Nicht erkannte Angriffe (sowohl interne durch andere Cloud-Nutzer als auch externe) oder keine zeitnahe Reaktion auf Angriffe; Verletzung der Vertraulichkeit von Informationen durch unbefugten Zugriff (auch z.B. von Administratoren)						Das verbleibende Risiko erscheint als so gering, dass das Betriebsrisiko hinsichtlich der genannten Gefährdung als tragbar erscheint.
Maßnahmen:						
41 24/7 umfassende Überwachung der Cloud Dienste sowie zeitnahe Reaktion bei Angriffen bzw. Sicherheitsvorfällen	x			1-8	Entsprechend seiner Notfallrichtlinie verfügt Ex Libris über ein 24/7-Überwachungssystem, inkl. Erfassung der System- und Zugangsprotokolle und einem Notfallmanagement-Team (s. Beschreibung in Kap. 10.1.8; Anlagen 5, 7 und 8); (s.a. Alma EVB-IT-Vertrag, Anlagen 3 und 7c).	
42 Erfassung und Auswertung von Datenquellen (z.B. Systemstatus, fehlgeschlagene Authentisierungsversuche, etc.)	x			1-8	s.o. # 41	
43 24/7-erreichbares, handlungsfähiges Team für Security Incident Handling und Trouble-Shooting			x	1-8	s.o. # 41	

n

Gefahrenszenarium und korrespondierende Maßnahmen	Grundbedrohung: Vertraulichkeit Verfügbarkeit Integrität	hohe Vertraulichkeit	hohe Verfügbarkeit	Bedrohte Daten	Sicherheitsmaßnahmen im Einzelnen	Risikobewertung unter Einbeziehung der Sicherheitsmaßnahme
44 Mitteilungspflichten des CSP gegenüber dem Kunden über Sicherheitsvorfälle oder Hinweise auf Sicherheitsvorfälle, die den Kunden betreffen könnten	x			1-8	Ex Libris informiert seine Kunden über Sicherheitsvorfälle(s. Beschreibung in Kap. 10.3; Anlage 5); (s.a. Alma EVB-IT-Vertrag, Anlagen 3 und 7a).	
45 Geeignete Bereitstellung relevanter Logdaten durch den CSP	x			1-8	s.o. # 44	
46 Logging und Monitoring der Aktivitäten von Administratoren	x			1-8	s.o. # 41	
K. Notfallmanagement Mögliche Gefährdungen ergeben sich z.B. durch: Unterbrechung bzw. Ausfall kritischer Geschäftspozesse z.B. durch Stromausfall, fehlerhafte Wartungsarbeiten oder Naturereignisse						Das verbleibende Risiko erscheint als so gering, dass das Betriebsrisiko hinsichtlich der genannten Gefährdung als tragbar erscheint.
Maßnahmen:						
47 Der Cloud-Anbieter muss ein Notfallmanagement aufsetzen und betreiben	x			1-8	Ex Libris besitzt einen Notfallplan inkl. Beschreibung Notfallrisiken und Präventivmaßnahmen, Backup- und Wiederherstellungsstrategien sowie eine Notfallrichtlinie für seine Cloud-Dienste (s. Kap. 10.1.9; Anlagen 5 und 7); (s.a. Alma EVB-IT-Vertrag, Anlage 7c).	
48 Der Cloud-Anbieter muss seinen Kunden die Priorisierung des Wiederanlaufs für die angebotenen Cloud-Dienste transparent machen			x	1-8	s.o. # 47	
49 Regelmäßige Notfall-Übungen (z.B. zu Ausfall eines Cloud Computing Standorts)			x	1-8	s.o. # 47	

Gefahrenszenarium und korrespondierende Maßnahmen	Grundbedrohung: Vertraulichkeit Verfügbarkeit Integrität	Grundbedrohung: hohe Vertraulichkeit	Grundbedrohung: hohe Verfügbarkeit	Bedrohte Daten	Sicherheitsmaßnahmen im Einzelnen	Risikobewertung unter Einbeziehung der Sicherheitsmaßnahme
50 Der Cloud-Anbieter sollte nachweisen, dass sein Notfallmanagement auf einem international anerkannten Standard wie z.B. BS 25999 oder BSIStandard 100-4 basiert (z.B. anhand Notfallvorsorgekonzept und Notfallhandbuch)			x	1-8	Ex Libris hat umfangreiches NotfallmanagementProgramm (s. u.a. #1-5 und #47; Kap. 10; Anlagen 5 und 7). Der Notfallplan (Business Continuity Plan) von Ex Libris (s. Anlage 7) enthält u.a. eine Analyse der Notfallrisiken und Präventionsmaßnahmen, Regelungen zur Notfallfeststellung und -klassifizierung, Wiederherstellungsstrategie, regelmäßige, jährliche Überprüfung und Aktualisierung, Notfallplanübungen. Ex Libris hat eine Notfallrichtlinie (s. Anlage 5) und ein eigenes Notfallmanagement-Team. Damit ist die Vergleichbarkeit zu Standards wie BS 25999 oder BSIStandard 100-4 gegeben. Ex Libris ist nicht nach BS 25999 oder BSI-Standard 100-4 zertifiziert, plant aber die Orientierung seines Notfallplans an den ISO 23001-Standard (der BS 25999 ersetzt hat). 2017 soll eine Bewertung vor-genommen und entschieden werden, ob der Notfallplan (Business Continuity Plan) im Laufe des Jahres 2018 nach ISO 23001 ausgerichtet werden kann.	
L. Portabilität und Interoperabilität Mögliche Gefährdungen ergeben sich z.B. durch: Datenverlust bei Wechsel zu einem anderen Service-Anbieter (Vendor Lock-In)						Das verbleibende Risiko erscheint als so gering, dass das Betriebsrisiko hinsichtlich der genannten Gefährdung als tragbar erscheint.
Maßnahmen:						
51 Exit-Vereinbarung mit zugesicherten Formaten	x			1-8	Bei Kündigung stellt Ex Libris seinen Kunden ihre Daten	

Gefahrenszenarium und korrespondierende Maßnahmen	Grundbedrohung: Vertraulichkeit Verfügbarkeit Integrität	hohe Vertraulichkeit	hohe Verfügbarkeit	Bedrohte Daten	Sicherheitsmaßnahmen im Einzelnen	Risikobewertung unter Einbeziehung der Sicherheitsmaßnahme
unter Beibehalten aller logischen Relationen und ggf. Offenlegung der damit verbundenen Kosten					in einem Standardformat zur Verfügung (s. Beschreibung in Kap. 10.1.10); (s.a. Alma EVB-ITVertrag, Anlage 3).	
52 Standardisierte oder offen gelegte Schnittstellen (API und Protokolle)	x			1-8	Ex Libris nutzt Standardprotokolle und –schnittstellen (s. Kap. 10.1.10)	
M. Sicherheitsprüfung und -nachweis Mögliche Gefährdungen ergeben sich z.B. durch: Angriffe aufgrund eines nicht mehr ausreichenden oder veralteten IT-Sicherheitszustand s der Geschäftsprozesse, Dienste oder Plattformen beim CSP oder dem Unterauftragnehmer						Das verbleibende Risiko erscheint als so gering, dass das Betriebsrisiko hinsichtlich der genannten Gefährdung als tragbar erscheint.
Maßnahmen:						
53 Cloud Service Anbieter müssen den Cloud- Nutzern regelmäßig über Sicherheitsmaßnahmen, Änderungen im IT-Sicherheitsmanagement, Sicherheitsvorfälle, die Ergebnisse durchgeführter IS-Revisionen und Penetrationstests berichten	x			1-8	Ex Libris informiert seine Kunden über Sicherheitsvorfälle und stellt seinen Kunden u.a. Imformationen zu Sicherheitsempfehlungen und Sicherheitsimplementierungen zur Verfügung (s.a. # 44; Beschreibung in Kap. 10.1.11; Anlage 5); (s.a. Alma EVB-IT-Vertrag, Anlage 7a).	
54 Regelmäßige Penetrationstests	x			1-8	Ex Libris nutzt ein Colacation-Rechenzentrum von Equinix, in dem regelmäißige Sicherheitsprüfungen von einer unabhängigen Prüfstelle durchgeführt werden (s. Beschreibung in Kap. 10.1.2; Anlage 4); (s.a. Alma EVBIT-Vertrag, Anlage 7c).	
55 Regelmäßige Penetrationstests bei Subunternehmen	x			1-8	s.o. # 54	

n

Gefahrenszenarium und korrespondierende Maßnahmen	Grundbedrohung: Vertraulichkeit Verfügbarkeit Integrität	hohe Vertraulichkeit	hohe Verfügbarkeit	Bedrohte Daten	Sicherheitsmaßnahmen im Einzelnen	Risikobewertung unter Einbeziehung der Sicherheitsmaßnahme
56 Regelmäßige und unabhängige Sicherheits revisionen		x		5,6,7,8	s.o. # 54	
			x	1-8		
57 Regelmäßige und unabhängige Sicherheits revisionen bei Subunternehmern		x		5,6,7,8	s.o. # 54	
			x	1-8		
N. Anforderungen an das Personal Mögliche Gefährdungen ergeben sich z.B. durch: Verletzung der Informationssicherheit, des Datenschutzes oder unsachgemäßer Umgang mit den Kundendaten; Fehlkonfigurationen mit gravierenden Folgen (z.B. hinsichtlich eingesetzter Techniken, Funktionalitäten oder Sicherheitsaspekten)						Das verbleibende Risiko erscheint als so gering, dass das Betriebsrisiko hinsichtlich der genannten Gefährdung als tragbar erscheint.
Maßnahmen:						
58 Vertrauenswürdiges Personal	x			1-8	Ex Libris unterzieht neue Mitarbeiter_innen einer Sicherheitsprüfung (s. Beschreibung in Kap. 10.1.12); (s.a. Alma EVB-IT-Vertrag, Anlage 7c).	
59 Ausbildung der Mitarbeiter des Cloud Service Anbieters (Regelmäßige Schulungen)	x			1-8	Ex Libris führt regelmäßige Sicherheitsschulungen und -sensibilisierungen durch (s. Beschreibung in Kap. 10.1.12); (s.a. Alma EVB-IT-Vertrag, Anlage 7c).	
60 Sensibilisierung der Mitarbeiter des Cloud Service Anbieters für Informationssicherheit und Datenschutz	x			1-8	s.o. # 59	
61 Verpflichtung der Mitarbeiter auf Informationssicherheit, Datenschutz, angemessenem Umgang mit Kundendaten	x			1-8	s.o. # 59	

Gefahrenszenarium und korrespondierende Maßnahmen	Grundbedrohung: Vertraulichkeit Verfügbarkeit Integrität	hohe Vertraulichkeit	hohe Verfügbarkeit	Bedrohte Daten	Sicherheitsmaßnahmen im Einzelnen	Risikobewertung unter Einbeziehung der Sicherheitsmaßnahme
O. Transparenz Mögliche Gefährdungen ergeben sich z.B. durch: Zugriff staatlicher Stellen auf die Daten aufgrund gesetzlicher Rahmenbedingungen des Landes, in dem die Daten gespeichert werden; Kosten durch Rechtsstreitigkeiten um Lizenzabgaben oder Patente; Einstellung des Dienstes oder Vertragskündigung bei Besitzerwechsel						Das verbleibende Risiko erscheint als so gering, dass das Betriebsrisiko hinsichtlich der genannten Gefährdung als tragbar erscheint.
Maßnahmen:						
62 Offenlegung der Standorte des Cloud Service Anbieters (Land, Region), an denen die Kundendaten gespeichert und verarbeitet werden	x			1-8	Ex Libris hat die Adressen seiner Speicherzentren bekannt gegeben (s. Kap. 10.1.2); (s.a. Alma EVB-ITVertrag, Anlage 7a).	
63 Offenlegung der Subunternehmer des Cloud Service Anbieters, die für die Erbringung der Cloud Services wesentlich sind	x			1-8	s. Alma EVB-IT-Vertrag, Anlage 7a	
64 Transparenz, welche Eingriffe der Cloud Service Anbieter oder Dritte in Daten und Verfahren der Kunden vornehmen dürfen	x			1-8	s. Alma EVB-IT-Vertrag, Anlage 7a	
65 Regelmäßige Unterrichtung über Änderungen (z.B. neue oder abgekündigte Funktionen, neue Subunternehmer, andere Punkte, die für das SLA relevant sind)	x			1-8	s. Alma EVB-IT-Vertrag	
66 Transparenz, welche Software durch den Cloud Service Anbieter aufseiten des Kunden installiert wird sowie über die daraus resultierenden Sicherheitserfordernisse/-risiken	x			1-8	Alma ist eine webbasierte Lösung und erfordert keine Softwareinstallation aufseiten des Kunden (s. Alma EVB-IT-Vertrag).	

Gefahrenszenarium und korrespondierende Maßnahmen	Grundbedrohung: Vertraulichkeit Verfügbarkeit Integrität	Grundbedrohung: hohe Vertraulichkeit	Grundbedrohung: hohe Verfügbarkeit	Bedrohte Daten	Sicherheitsmaßnahmen im Einzelnen	Risikobewertung unter Einbeziehung der Sicherheitsmaßnahme
67 Transparenz bezüglich staatlicher Eingriffs- und Einsichtrechte, über gerichtlich festlegbare Einsichtrechte Dritter und über Prüfpflichten zu gespeicherten Daten durch den Cloud Service Anbieter an allen potenziellen Standorten	x			1-8	s. Alma EVB-IT-Vertrag, Anlage 7a-c	
68 Darlegung der Rechts- und Besitzverhältnisse des Cloud Service Anbieters sowie der Entscheidungsbefugnisse	x			1-8	Beschreibung durch Ex Libris s. Anlage 2	
P. Service Level Agreement (SLA) Mögliche Gefährdungen ergeben sich z.B. durch: Unzureichende Leistungen und unzureichende Sicherheitsmaßnahmen; nicht gelöschte Daten gelangen nach Vertragsende „in die falschen Hände"; Verlust der Verfügbarkeit der Anwendung oder der Vertraulichkeit der Daten aufgrund von Insolvenz						Das verbleibende Risiko erscheint als so gering, dass das Betriebsrisiko hinsichtlich der genannten Gefährdung als tragbar erscheint.
Maßnahmen:						
69 Definierte Sicherheitsleistungen durch Security-SLA oder im SLA deutlich hervorgehoben	x			1-8	Ex Lbiris hat ein Verfahren der Schwachstellenanalyse und implementiert Patches schnellstmöglich (s. Beschreibung in Kap. 10.1.3 und 10.1.4; Anlage 8); (s. Alma EVB-IT-Vertrag, Anlage 7a-c).	
70 Sicherstellung des Betriebs oder der Bereit-stellung der Daten im Falle einer Insolvenz des Cloud Service Anbieters unter Beachtung von Vertraulichkeits-zusagen und Datenschutzanforderungen		x		5,6,7,8	s.o. # 51	
			x	1-8		

n

Gefahrenszenarium und korrespondierende Maßnahmen	Grundbedrohung: Vertraulichkeit, Verfügbarkeit, Integrität	Grundbedrohung: hohe Vertraulichkeit	Grundbedrohung: hohe Verfügbarkeit	Bedrohte Daten	Sicherheitsmaßnahmen im Einzelnen	Risikobewertung unter Einbeziehung der Sicherheitsmaßnahme
Q. Datenschutz und Compliance Mögliche Gefährdungen ergeben sich z.B. durch: Datenschutzverletzungen; Verletzung sonstiger rechtlicher Bestimmungen						Das verbleibende Risiko erscheint als so gering, dass das Betriebsrisiko hinsichtlich der genannten Gefährdung als tragbar erscheint.
Maßnahmen:						
71 Gewährleistung des Datenschutzes nach deutschem Recht	x			1-8	s. Alma EVB-IT-Vertrag, Anlage 7a	
72 Datenschutzrichtlinien und –gesetze, denen der Cloud-Nutzer unterliegt, müssen eingehalten werden	x			1-8	s. Alma EVB-IT-Vertrag, Anlage 7a	
73 Bei Auftragsdatenverarbeitung: Schriftliche Vereinbarung zwischen Cloud-Nutzer und CloudAnbietern gemäß § 11 Abs. 2 BlnDSG mit Mindestinhalt nach § 11 Abs. 2 Satz 2 BlnDSG, u.a.: » Beschreibung von Gegenstand und Dauer des Auftrags » Genaue Bezeichnung der Erhebung, Verarbeitung und Nutzung personenbezogener Daten » Festlegung der technischen und organisatorischen Maßnahmen: Festlegung des genauen Ortes der Verarbeitung personenbezogener Daten beim Cloud-Anbieter einschließlich der technischen und organisatorischer Verarbeitungsumgebung	x			1-8	s. Alma EVB-IT-Vertrag, Anlage 7a	

Gefahrenszenarium und korrespondierende Maßnahmen	Grundbedrohung: Vertraulichkeit, Verfügbarkeit, Integrität	Grundbedrohung: hohe Vertraulichkeit	Grundbedrohung: hohe Verfügbarkeit	Bedrohte Daten	Sicherheitsmaßnahmen im Einzelnen	Risikobewertung unter Einbeziehung der Sicherheitsmaßnahme
» Umgang mit Ansprüchen Betroffener auf Berichtigung, Sperrung und Löschung personenbezogener Daten » Einhaltung von § 11 Abs. 4 BlnDSG » Festlegung oder Verbot etwaiger Unterauftragsverhältnisse » Kontrollrechte des Cloud-Nutzers » Weisungsbefugnisse des Cloud-Nutzers » Rückgabe bzw. Löschung von Daten nach Beendigung des Auftrags						
74 Bei Übermittlung und Auftragsdaten-verarbeitung: Speicherung und Verarbeitung der personenbezogenen Daten » innerhalb der Mitgliedstaaten der EU oder Vertragsstaats des EWR (Europäischen Wirtschaftsraums) oder » außerhalb der EU oder eines Vertragsstaats des EWR, wenn ein angemessenes Datenschutzniveau gewährleistet werden kann, z.B. durch: - Entscheidung der EU-Kommission - Beitritt zum Safe-Harbour-Agreement (USA) - EU-Standardvertragsklauseln - Genehmigung der Aufsichtsbehörde	x			1-8	s. Alma EVB-IT-Vertrag, Anlage 7a	

n

Gefahrenszenarium und korrespondierende Maßnahmen	Grundbedrohung: Vertraulichkeit Verfügbarkeit Integrität	Grundbedrohung: hohe Vertraulichkeit	Grundbedrohung: hohe Verfügbarkeit	Bedrohte Daten	Sicherheitsmaßnahmen im Einzelnen	Risikobewertung unter Einbeziehung der Sicherheitsmaßnahme
75 Keine Einbindung von Unterauftragnehmern, die eine Verarbeitung der personenbezogenen Daten unter den oben genannten Voraussetzungen nicht gewährleisten können	x			1-8	s. Alma EVB-IT-Vertrag, Anlage 7a	
76 Kontrollrechte des Kunden zur datenschutzkonformen Verarbeitung der personenbezogenen Daten bei der Auftragsdatenverarbeitung durch » Vor-Ort-Kontrolle oder » Testat eines unabhängigen Sachverständigen	x			1-8	s. Alma EVB-IT-Vertrag, Anlage 7a	
77 Bei Auftragsdatenverarbeitung: Kontrollrecht der für den Cloud-Nutzer zuständigen Aufsichts-behörde	x			1-8	s. Alma EVB-IT-Vertrag, Anlage 7c	
78 Bei Auftragsdatenverarbeitung: Weisungsrechte des Cloud-Nutzers gegenüber dem Cloud-Anbieter	x			1-8	s. Alma EVB-IT-Vertrag, Anlage 7a	
79 Für den Cloud-Nutzer relevante gesetzliche Bestimmungen müssen durch den Anbieter eingehalten werden	x			1-8	s. Alma EVB-IT-Vertrag, Anlage 7a	

8. Rechtemanagement

8.1 Benutzer_innen in Alma

8.1.1 Interne und externe Benutzer_innen (Internal / External User)

In Alma werden je nach dem Quellsystem der Daten folgende Arten von Benutzer_innen unterschieden:

- interne Benutzer_innen (Internal User) und
- externe Benutzer_innen (External User)

Interne Benutzer_innen werden in Alma angelegt und komplett in Alma verwaltet. Externe Benutzer_innen werden außerhalb von Alma im universitätseigenen System (z.B. dem IDM einer Universität) gepflegt und über eine Schnittstelle aktualisiert.

➢ Weiteres in Anlage 1 – jeweiliger universitätsspezifischer Teil

8.1.2 Mitarbeiter_innen (Staff User) und Benutzer_innen (Patron)

Entsprechend ihrem Status in Bezug zur Bibliothek gibt es in Alma weiterhin die Unterscheidung zwischen

- Mitarbeiter_innen (Staff User) sowie
- Benutzer_innen (Patrons)

Mitarbeiter_innen sowie Benutzer_innen (Patrons) können sowohl interne als auch externe Benutzer_innen (Internal bzw. External User) sein.

8.2 Authentifizierung und Autorisierung in Alma

Alma unterscheidet zwischen Authentifizierung und Autorisierung.

8.2.1 Authentifizierung

Bei der Authentifizierung kommt die Unterscheidung in interne und externe Benutzer_innen zum Tragen.

Die Authentifizierung der **internen Benutzer_innen** erfolgt in Alma. Dazu sind die Zugangspasswörter in Alma gespeichert. Die Passwörter werden nach Regex konfiguriert und müssen folgende Regeln erfüllen:

- mindestens 8 Zeichen und maximal 20 Zeichen lang
- mindestens ein Buchstabe (Klein- oder Großbuchstabe)
- mindestens eine Ziffer
- mindestens ein Sonderzeichen - Erlaubt sind die Sonderzeichen ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ { } ~
- keine Leerzeichen am Anfang oder am Ende des neuen Passwortes

Die Authentifizierung der **externen Benutzer_innen** erfolgt über Shibboleth bzw. LDAP im universitätseigenen IDM. Dort werden auch die Passwörter gespeichert und verwaltet. Alma kennt die Passwörter der externen Benutzer_innen nicht.

8.2.2 Autorisierung

Die Autorisierung erfolgt – nach erfolgreicher Authentifizierung – immer in Alma und immer rollenbasiert. Eine Rolle, die Berechtigungen, die sie enthält, der Umfang der Rolle und deren Ablaufdatum legen die Autorisierung für jede Aktion fest. Das Rollen- und Rechtekonzept ist nachfolgend beschrieben.

8.3 Rollen- und Rechtekonzept in Alma

8.3.1 Die Rolle „Patron"

Die Rolle „Patron" ist in Alma mit Rechten verbunden, die auf einem spezifischen Status basieren (z.B. Studierende, Professor_innen usw.). Abhängig vom Status werden die Patrons einer Alma-Benutzergruppe zugeordnet. Die Alma-Benutzergruppen werden von den dazu autorisierten Mitarbeiter_innen entsprechend den Benutzungsrichtlinien der Bibliothek eingerichtet und mit Berechtigungen versehen (z.B. spezifische Ausleihkonditionen für Professor_innen). Neu hinzukommende Patrons, die den gleichen Status haben, erhalten dann automatisch dieselben Rechte.

8.3.2 Rollen und Rechte für Mitarbeiter_innen

Mitarbeiter_innen haben in Alma unterschiedliche Rollen und Rechte, um ihre Aufgaben in der Bibliothek zu erledigen. Die Zuordnung von **Rollen** erfolgt in Alma über sogenannte Arbeitsfelder. Entsprechend dem spezifischen Aufgabengebiet in der Bibliothek werden jeder/m Mitarbeiter_in Alma-Arbeitsfelder zugeordnet. Jedes Arbeitsfeld enthält eine Rollenvorlage (Template) mit Gruppen von Rollen, die je nach Aufgabengebiet dem/der Mitarbeiter_in zugeordnet werden können. Die meisten Rollenvorlagen sind von Ex Libris vorformuliert; neue Templates können angelegt werden. Dies ist insofern von Vorteil, als es in der Bibliothek Mitarbeiter_innen gibt, die gleiche Aufgabengebiete und gleiche Rollen haben. Mit Hilfe der Templates muss nicht jede Rolle für jedes Aufgabengebiet individuell erstellt werden.

Die Rollen sind in Alma festgelegt. Jede Rolle ist mit bestimmten **Rechten** verknüpft, welche Aktionen der/die Mitarbeiter_in in Alma ausführen kann. Eine Übersicht über die Rollen in Alma und die damit verbundenen Rechte steht in Anlage 3.

8.3.3 Spezielle Beschränkungen

Bestimmte Berechtigungen sind nicht allein an die Rollen geknüpft, sondern zusätzlich an die Voraussetzung, an bestimmten Arbeitsplätzen angemeldet zu sein oder einer definierten Arbeitsgruppe zuzugehören. Die Zuordnung/Steuerung erfolgt IP-basiert. So können z.B. Mitarbeiter_innen der Leihstelle Benutzerdienste nur bearbeiten, wenn Sie an einem PC der Leihstelle angemeldet sind. Ansonsten haben die Mitarbeiter_innen nur Sichtrechte. Durch diese Schutzmaßnahme wird verhindert, dass Mitarbeiter_innen von außerhalb des Arbeitsplatzes schreibenden Zugang zu personenbezogenen Daten haben, ohne dass dieser Zugriff zur Erfüllung dienstlicher Pflichten erforderlich ist.

Diese zusätzlichen Definitionsanforderungen gelten für die Rollen: Leihstellen- Mitarbeiter, Leihstellen- Mitarbeiter - eingeschränkt, Leihstellen-Manager, Bestellungen-Mitarbeiter,

Bearbeitungsauftrags-Mitarbeiter, Eingangs-Mitarbeiter, Eingangs-Mitarbeiter – eingeschränkt, Benutzungsservice-Mitarbeiter.

8.3.4 Prinzipien der Rollen- und Rechtezuordnung

Rollen werden nach der Maßgabe zugewiesen, dass die Rolleninhaber_innen die ihnen im Rahmen der Bedienung von Alma zugewiesenen Aufgaben erfüllen können müssen, um ihre spezifischen Arbeiten in der Bibliothek zu erledigen. Sie sollen aber nicht über Rechte zur Durchführung von Aufgaben verfügen, die nicht zu ihrem Aufgabengebiet gehören. So legitimieren zum Beispiel Gründe der Vereinfachung der Benutzerverwaltung keine Vereinheitlichung von Rechten ohne Blick auf das übertragene Aufgabenspektrum.

8.3.5 Festlegungen der Bibliotheken für die Rollenvergabe

- Weiteres in Anlage 1 – jeweiliger universitätsspezifischer Teil

8.4 Aktionen in Alma im Hinblick auf personenbezogene Daten

- Weiteres in Anlage 1 – jeweiliger universitätsspezifischer Teil

8.5 Verwaltung der internen Benutzer_innen

- Weiteres in Anlage 1 – jeweiliger universitätsspezifischer Teil

8.6 Verwaltung der externen Benutzer_innen

- Weiteres in Anlage 1 – jeweiliger universitätsspezifischer Teil

8.7 Anonymisierung/Löschung von Benutzer_innen in Alma

8.7.1 Anonymisierung/Löschung

In Alma können drei Benutzer-Lösch-Konfigurationen unterschieden werden:

- **Vollständig ausweisbar beibehalten** – Der Status des/r Benutzer_in ist **Gelöscht**; alle Bestellungen werden storniert und die identifizierende Zeichenfolge wird deaktiviert. Die übrigen Daten des/r Benutzer_in werden im System beibehalten. Damit ist der Nutzer anonymisiert und es können keine personenbezogenen Auswertungen in Analytics erfolgen.

  Dies ist die Standard-Einstellung, wenn Benutzer_innen in Institutionen erstellt werden, die zuvor mit Alma konfiguriert wurden.

- **Statistik beibehalten** – Die statistischen Daten des/r Benutzer_in werden beibehalten – das heißt, alle nicht-identifizierenden statistischen Daten (wie die Benutzergruppe und Prozesskategorie) werden beibehalten, sowie Daten in der Registerkarte **Statistik**. Alle anderen Daten werden gelöscht.

Dies ist die Standard-Einstellung, wenn Benutzer_innen in Institutionen erstellt werden, die neu mit Alma konfiguriert wurden.

- **Vollständig entfernen** – Entfernt bei der Löschung alle Benutzerdaten, einschließlich statistischer Daten.

Im Regelfall wird zur Löschung angewendet: Statistik beibehalten.

Bei Ex Libris gelten auf der Grundlage des DoD 5220.22-M-Standards für das Löschen und Bereinigen von Daten auf beschreibbaren Datenträgern strenge Verfahren und Richtlinien für den Umgang mit obsoleten entfernbaren Daten. Diese Verfahren gelangen auch dann zur Anwendung, wenn ein Kunde sich zu einer Kündigung des Dienstes entschließt. Disketten und Bänder werden vernichtet, sobald sie nicht länger benötigt werden. CDs, die nicht länger benötigt werden, werden mittels eines CD/DVD-Vernichters oder Shredders vernichtet. Alle Speichergeräte, die gegebenenfalls wiederverwendet werden sollen, werden durch eine Datenbereinigungssoftware bereinigt.

➢ Weiteres in Anlage 1 – jeweiliger universitätsspezifischer Teil

8.7.2 Nutzung anonymisierter Ausleih-/Gebühren- und Benutzerdaten für Statistiken

Ausleih-, Gebühren- und Benutzerdaten werden in Alma nicht gelöscht, sondern anonymisiert, damit die Daten für Statistikzwecke weiterhin in Analytics auswertbar sind.

Die Bibliothek benötigt für die Planung, Steuerung und den Nachweis ihrer Arbeit längerfristig statistisch auswertbare Daten. Dies ist sowohl für die Planung des Personaleinsatzes, als auch für die Benutzungsdienste und für die Planung der Verwendung des Erwerbungsetats notwendig.

Die Bibliotheken erheben Daten für die Deutsche Bibliotheksstatistik (DBS), der nationalen Datenbasis zum Bibliothekswesen in Deutschland. Die DBS umfasst alle Bibliothekssparten und basiert auf einheitlichen Definitionen (ISO 2789 "Internationale Bibliotheksstatistik"). Das Zahlenmaterial und die Auswertungen werden für Bibliotheksentwicklungen, für die Einschätzung von Trends sowie für politische Argumentationen genutzt.

➢ Weiteres in Anlage 1 – jeweiliger universitätsspezifischer Teil

9. Beschreibung der IT-Komponenten (Seite Bibliothek)

➢ Weiteres in Anlage 1 – jeweiliger universitätsspezifischer Teil

II. Beschreibung Dienstleister

10. Erläuterung der Schutzmaßnahmen im Hinblick auf Vertraulichkeit, Verfügbarkeit und Integrität

10.1 Cloud-spezifische Maßnahmen

Die Firma Ex Libris hat anhand des BSI-Eckpunktepapiers (s. Kap. 1) sowie mehrerer Anlagen dargelegt, welche Sicherheitsmaßnahmen sie im SaaS-Dienst Alma einsetzt, um die Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Rückverfolgbarkeit und Transparenz im Hinblick auf die Verarbeitung personenbezogener Daten zu gewährleisten. Ex Libris beschreibt unter anderem die folgenden technischen und organisatorischen Maßnahmen:

10.1.1 Sicherheitsmanagement beim Anbieter

Ex Libris hat sichere Betriebsabläufe festgelegt und implementiert, einschließlich Änderungsmanagement, Notfallmanagement, Asset Management und Konfigurationsmanagement, basierend auf den ITIL-Best Practices. Die Grundsätze der „Mindestberechtigung" und des „begründeten Informationsbedarfs", Authentisierung, Sicherheitsanforderungen, Separierung, Isolation, Segregation und Sicherheitsmaßnahmen sind Teil der Betriebsabläufe. Die Firma hat im Rahmen der ISO 27001:2013 eine ISO-Prüfung bestanden, einschließlich Rechenzentrums-, globaler Betriebs- sowie Anwendungs- und Entwicklungsprozesse.

Ex Libris beschäftigt einen eigenen Sicherheitsbeauftragten, der Ansprechpartner für Sicherheitsfragen ist, einen Datenschutzbeauftragten für datenschutzrechtliche und regulatorische Fragen, sowie ein eigenes Sicherheitsteam, gemeinsam mit einem Cloud Services Team, das folgende Aufgaben wahrnimmt:

- Umsetzung des Sicherheitsmodells auf allen Systemebenen
- Überwachung und Analyse der Infrastruktur hinsichtlich verdächtiger Aktivitäten und potenzieller Gefahren
- Veröffentlichung regelmäßiger Sicherheitsberichte für die Geschäftsleitung und Kunden von Ex Libris
- Dynamische Aktualisierung des Sicherheitsmodells und Bewältigung neuer Sicherheitsgefährdungen

Die Dienste und Rechenzentren von Ex Libris sind ISO 27001:2013-zertifiziert. Die Firma verpflichtet sich zu einer jährlich von einem unabhängigen Drittunternehmen durchgeführten Sicherheitsprüfung. Darüber hinaus werden die Produkte von Ex Libris mindestens einmal jährlich den Sicherheitspenetrationstests eines unabhängigen Sicherheitsunternehmens unterzogen.

10.1.2 Physische Sicherheit in den Rechenzentren

Hardware, Netzwerk, Software und Daten von Ex Libris werden in folgender Weise physisch gesichert:

Ex Libris nutzt ein Colocation-Rechenzentrum im Eigentum von Equinix, einem globalen Anbieter von Rechenzentren. Als Colocation-Rechenzentrum stellt Equinix die Einrichtungen (Platz, Strom, Kühlung etc.) zur Verfügung, während die gesamte Computer-Infrastruktur (Firewalls, Netzwerk-Switches, Server, Speicherung etc.) im Eigentum von Ex Libris steht. Da Equinix nur Einrichtungen zur Verfügung stellt und keinen Zugriff auf die tatsächlich in den Servern gespeicherten Daten erhält, bestehen keine zusätzlichen rechtlichen Risiken oder Abhängigkeiten.

Die Rechenzentren von Equinix haben eine SSAE-16-Sicherheitszertifizierung [redacted] erhalten, als Ergebnis einer eingehenden Prüfung der Kontrollziele und Kontrollmaßnahmen der Zentren, einschließlich der Kontrollen über die Informationstechnologie und alle übrigen damit verbundenen Prozesse.

Die Sicherheitskontrollen in den Rechenzentren beruhen auf Standardtechnologien. Die physischen Zugangssicherheitskontrollen unterstützen eine Zwei-Faktor-Authentifizierung (something you know and something you have principles), einschließlich Biometrie- und Sicherheitscodeanforderungen. Sie sind so gestaltet, dass sie die Auswirkungen einzelner Schwachstellen eliminieren und die Ausfallsicherheit des Rechenzentrums bewahren. Der physische Zutritt zum Rechenzentrum ist auf Personen beschränkt, die aus betrieblichen Gründen Zugang zur Infrastruktur benötigen. Alle physischen Zugangsaktivitäten werden protokolliert und überwacht. Alle Besucher müssen vorab genehmigt werden und die Genehmigung gilt für einen begrenzten Zeitraum. Besucher müssen während ihres Aufenthaltes von einem autorisierten Mitarbeiter begleitet werden.

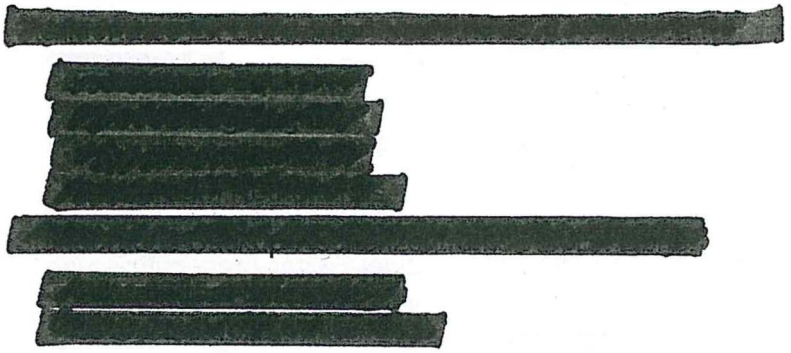
Jedes Equinix-Rechenzentrum verfügt über: Unterbrechungsfreie Stromversorgungssysteme (UPS) zur Verhinderung von Power Spikes, Überspannungen und Spannungsabfällen sowie redundante Backup-Dieselgeneratoren für eine zusätzliche Betriebsdauer. Ein robustes HVACSystem sorgt für eine stabile Luftzufuhr, Temperatur und Luftfeuchtigkeit, mit einer Redundanz von mindestens N+1 für alle Hauptgeräte.

- N+2 Redundanz für Kühlaggregate und Thermalenergiespeicherung, für eine verbesserte Temperaturstabilität.
- Branderkennung und -bekämpfung
- Erdbebenverankerungs- und -verstrebungssysteme
- Hochwasserschutz
- 24x7x365 Sicherheit
- Sicherung aller Türen, einschließlich der Cages, durch biometrische Handgeometrieleser
- CCTV-Digitalkameraüberwachung des gesamten Zentrums, einschließlich der Cages, mit detaillierten Überwachungs- und Prüfprotokollen
- Erfassung durch CCTV bei Zugang

Die physischen Sicherheitskontrollen sind unter Berücksichtigung von Brandschutzaspekten gestaltet, einschließlich Feuermeldesystem, Brandfrüherkennung, angemessener Brandbekämpfungsausstattung, regelmäßiger Brandschutzübungen [redacted].

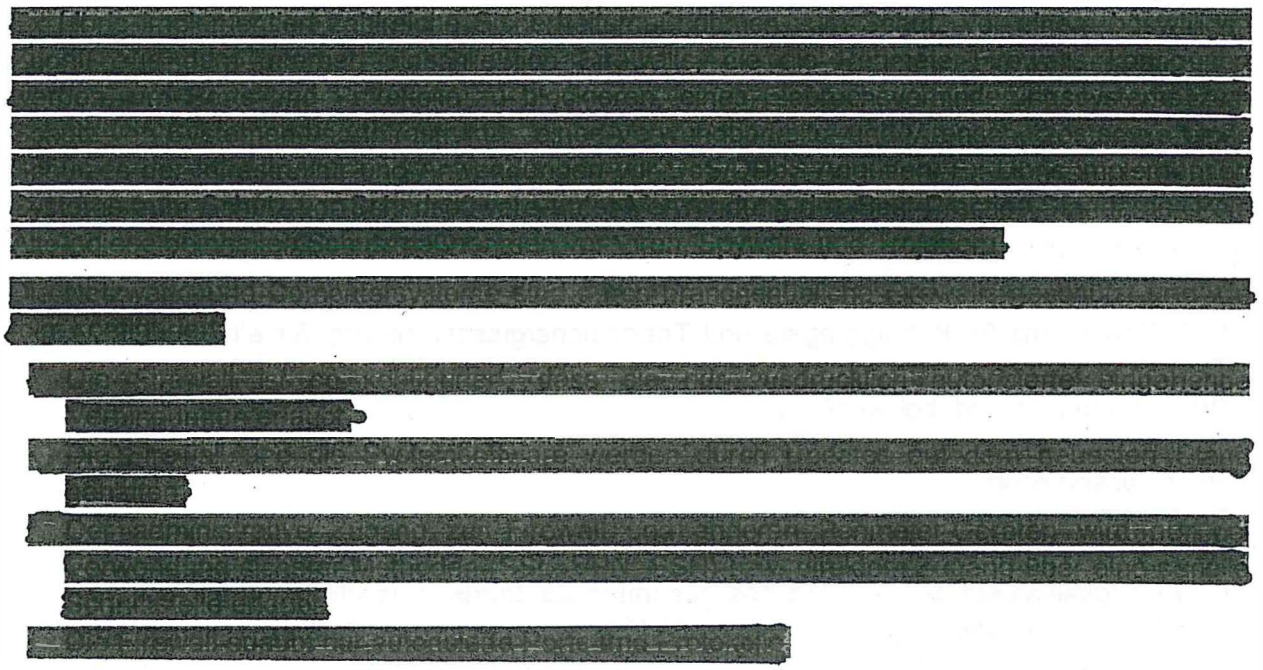
Die Cloud-Dienste für die europäischen (EU-)Kunden erfolgen aus dem EU-Rechenzentrum in Amsterdam, Niederlande. Im Rahmen der Verträge werden die Kunden über die Standorte der Rechenzentren sowie vorab über alle diesbezüglichen Änderungen informiert.

Ex Libris unterhält ein Offsite-Backup aller Kundendaten in einem externen, gesicherten Rechenzentrum in Zwolle, Niederlande - dieser Standort befindet sich über 100 Kilometer vom Hauptrechenzentrum in Amsterdam entfernt. Jeden Tag wird ein vollständiges tägliches Backup im externen Standort gespeichert. Im Fall einer Katastrophe im Hauptrechenzentrum ist Ex Libris so in der Lage, eine Wiederherstellung aus dem externen und gesicherten Disk-Backup durchzuführen.



Im Fall von Änderungen der obigen Anschriften informiert Ex Libris die Bibliothek unverzüglich.

10.1.3 Server-Sicherheit und Netzwerksicherheit



Auf der Grundlage der Best-Practices der Betriebs- und Anwendersicherheit hat Ex Libris sichere Host-Verfahren als Teil der Bereitstellung für die Installation neuer Server und Dienste implementiert. Ex Libris verifiziert die Einhaltung dieser Standards durch jährliche Prüfungen, Penetrationstests und Compliancеprüfungen.

Welche Regelungen und Verfahren zum Schutz vor Gefährdungen eingesetzt werden und wie Sicherheitsvorfälle bearbeitet und dokumentiert werden, wird in Anlage 5 erläutert.

- Alle Signatur- und Definitionsdateien werden täglich aktualisiert.
- Jeder als schädlich eingestufte Netzwerkverkehr wird blockiert.

- Nur autorisierte Protokolle und Ports dürfen die Firewall und das Netzwerk passieren. Allen übrigen wird der Zugang verwehrt.

Ex Libris verfügt über ein Verfahren zur Schwachstellenanalyse, einschließlich Bewertung und Definition des Schweregrades. Kritische Patches werden innerhalb von 5 Werktagen bewertet und schnellstmöglich implementiert. Ex Libris führt mindestens einmal jährlich externe und interne Penetrationstests sowie Schwachstellenanalysen durch, um potenzielle Verwundbarkeiten und Schwachstellen zu identifizieren, die für einen Missbrauch der Systeme genutzt werden könnten.

Alle Geräte, einschließlich der Hypervisoren, durchlaufen vor ihrer Implementierung in die Produktion ein Verfahren, das Änderungsmanagement und vollständige Qualitätsanalyse einschließt, mit halbjährlichen Scans (SANS Top 25) und jährlichen Penetrationstests. Ex Libris nutzt die Red Hat KVM (Kernel-based Virtual Machine) Community Edition, die eine EAL 4+ Zertifizierung besitzt.

Alle in der Cloud-Architektur eingesetzten Komponenten basieren auf einem festgelegten Sicherheitsstandard des Anbieters und Sicherheits-Best Practices und durchlaufen vor ihrem Einsatz in der Produktion einen Änderungskontrollprozess, einschließlich, Konfiguration, Test und Qualitätsanalyse.

10.1.4 Betriebssystem-Management und -Sicherheit

Die Abläufe für die Betriebssystemsicherheit werden rund um die Uhr vom Ex Libris Security Operation Center analysiert und bewertet. Das von Ex Libris betriebene Security Operation Center - auch als HUB bzw. NOC bezeichnet - protokolliert und überwacht alle logischen Netzwerkzugriffe auf Kundendaten und die Verwendung von Informationswerten und wird vom Sicherheitsbeauftragten von Ex Libris überprüft. Das Monitoring von Ex Libris besteht aus mehrschichtigen, vollständig redundanten Systemen, welche die Leistungen innerhalb und außerhalb des Rechenzentrums überwachen, um sicherzustellen, dass die Dienste auf dem höchsten Leistungsniveau betrieben werden.

Die von der Ex Libris-Software genutzten Fremdbetriebssysteme erhalten Sicherheits-Updates und aktuell unterstützte Versionen vom Hersteller. Alle Sicherheits-Updates auf der Betriebssystemebene (OS, Gerätetreiber etc.) und auf der Anwendungsebene (Datenbanken, Anwendungen etc.) werden auf dem neuesten Stand gehalten. Ex Libris verfügt über ein Verfahren zur Implementierung von Patches, Updates und Service Packs, das eine Verifizierung und Erprobung von Änderungen vor deren Freigabe beinhaltet.

Systemzugangspasswörter von Betriebssystemen unterliegen der Passwortrichtlinie von Ex Libris, die Regelungen für die Validierung, die Stärke und die Historie/Wiederverwendung von Passwörtern festlegt (siehe Anlage 6).

Der Zugang zum Betriebssystem für Maßnahmen der Fernadministration ist begrenzt auf zugelassene Nutzer und Ursprungsorte. Sowohl für die Authentisierung als auch die Session werden die Secure Tunnel- oder SSH-Remote-Verbindungen mit mindestens einer 256-bitVerschlüsselung verwendet.

Für die Produkte erfolgt eine Sicherheitsprotokollierung der nachstehenden erfolgreichen bzw. fehlgeschlagenen Versuche: Authentisierungen; Operationen des Nutzermanagements (z.B.

Nutzererstellung und Änderung von Passwörtern); sowie Zugangskontrolländerungen (Änderungen der Freigabe für kritische Systeme und Anwendungskomponenten).

Die Protokolle von Sicherheitsvorfällen enthalten mindestens folgende Angaben: Nutzer-ID; Datum und Uhrzeit der Ausführung; Angabe ob erfolgreich oder nicht; Ausgangspunkt der Ausführung; Identität der betroffenen Ressource.

Alle Protokolle von Sicherheitsvorfällen werden täglich einheitlich analysiert und bewertet. In der Cloud-Umgebung wird eine Antiviren-Software eingesetzt. Die Virensignaturen werden täglich aktualisiert.

10.1.5 Anwendungs- und Plattformsicherheit

Die Produkte von Ex Libris folgen dem Agile System Development Life Cycle (SDLC – Systementwicklungs-Lebenszyklus). Dies erlaubt es Ex Libris, eine mandantenfähige, cloudbasierte SaaS mit monatlichen Releases anzubieten, sowie schneller auf Kundenbedürfnisse, einschließlich Sicherheitsaspekte, zu reagieren. Sichere Codierungsverfahren und ein Sicherheitsbewusstsein sind integrale Bestandteile des SDLC-Programms von Ex Libris. Darüber hinaus verfügt Ex Libris über ein eigenes Sicherheitsteam, das bei jedem ReleaseZyklus Sicherheitsprüfungen und Verwundbarkeitsbewertungen durchführt sowie jährliche externe Penetrationstests, einschließlich mindestens der OWASP Top 10 und SANS Top 25 Sicherheits-, Verwundbarkeits- und Minderungspläne.

Im Rahmen der Richtlinien von Ex Libris zum Entwicklungs-Lebenszyklus werden vom Teamleiter bzw. Code-Verfasser Prüfungen durchgeführt. Tests der Codeprüfungen erfolgen durch den Sicherheitsbeauftragten, welcher mindestens vierteljährlich einen Sicherheitsprüfung und Schwachstellenanalyse durchführt - zusätzlich zu einem jährlichen AnwendungsPenetrationstest zur Verifizierung der Umsetzung der Sicherheitsmaßnahmen.

Ex Libris hat Änderungsmanagement-Abläufe eingerichtet, so dass alle Tätigkeiten protokolliert, dokumentiert, geplant und genehmigt werden. Der Sicherheitsbeauftragte von Ex Libris validiert die angewandten Verfahren und im Rahmen des ISO-Prüfungs- und Zertifizierungsverfahrens wird überprüft, dass alle Sicherheitsmaßnahmen umgesetzt wurden.

Es werden Verfahren eingesetzt, die eine Anwendung sperren, wenn ein Mitarbeiter bzw. ein Mitarbeiter eines Dienstleisters gekündigt wird oder das Unternehmen verlässt.

Das Entwicklungsteam von Ex Libris ist im Umgang mit Sicherheitsprogrammierungstechniken geschult, so dass häufige Verwundbarkeiten identifiziert und vermieden werden können, z.B. im „Top Ten-Projekt“ des Open Web Application Security Project (OWASP). Ex Libris setzt auch Anwendungsentwicklungsprozesse nach ISO 27001:2013 für den SoftwareentwicklungsLebenszyklus ein. [redacted] Ex Libris führt Schulungen zu Datenschutz- und Sicherheitsaspekten durch, die im Rahmen der ISO-Zertifizierung geprüft werden. Die Prüfung validiert, dass alle Mitarbeiter in den Bereichen allgemeine Informationssicherheit, Sicherheitscodes, Schutz von Kundendaten und Meldung verdächtiger Aktivitäten an den Sicherheitsbeauftragten von Ex Libris geschult sind.

Der Sicherheitsbeauftragte von Ex Libris ist zuständig für die Sicherheit der Software insgesamt während ihrer Entwicklung, des Managements und des Betriebes. Ex Libris verfügt über gut dokumentierte Verfahren und Bedingungen zur Ausführung von Codeanalysen.

Ex Libris verwendet ein Tool zur Schwachstellenanalyse im Rahmen des Softwareentwicklungsprozesses, um häufige Programmierungsfehler erkennen zu können. Dieses Tool erkennt mindestens alle in der aktuellen Top Ten-Liste von OWASP aufgeführten Schwachstellen.

10.1.6 Datensicherheit

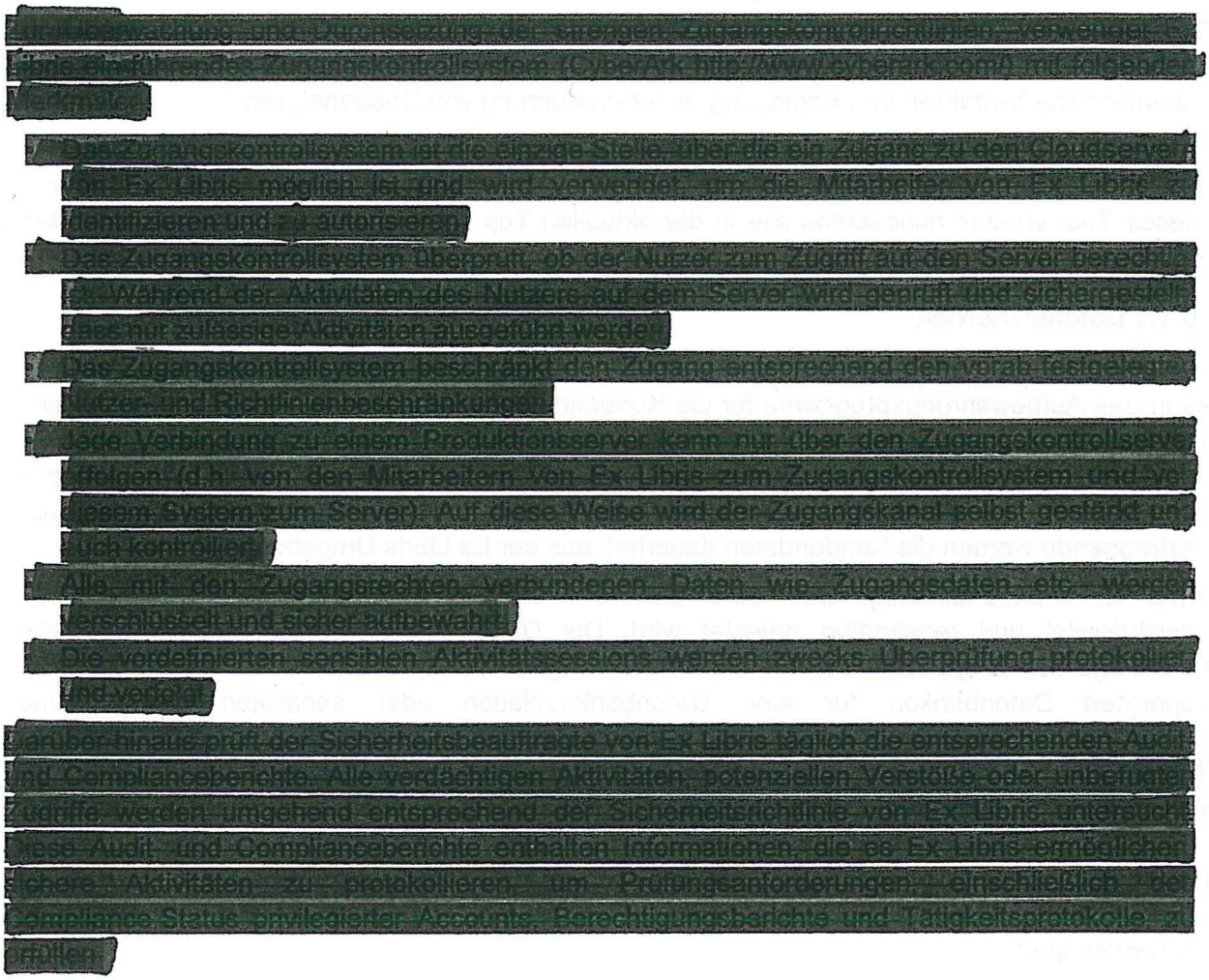
Der Kunde behält die vollständige Kontrolle über die im SaaS-Dienst gespeicherten Daten und kann das Aufbewahrungsprogramm für die Kundendaten bestimmen. Der Vertrag von Ex Libris sieht vor, dass die Kundendaten bei Beendigung bzw. Abschluss der Leistung (kostenfrei) zum Download bereitstehen. Der Kunde hat 30 Tage Zeit, die Daten herunterzuladen, bevor diese von Ex Libris gelöscht werden. Auf Wunsch bestätigt Ex Libris die Löschung der Daten. Nach Vertragsende werden die Kundendaten dauerhaft aus der Ex Libris-Umgebung gelöscht.

Alma ist mandantenfähig, was eine sichere Trennung der kundenspezifischen Daten gewährleistet und regelmäßig getestet wird. Die Datenisolation erfolgt entweder auf der Grundlage von Gruppenlaufwerken, die Firewall-Regeln für eine Netzwerkisolation verwenden, separaten Datenbanken für eine Datenbank-Isolation oder separaten Dateien und Berechtigungen für eine Filesharing-Isolation. [redacted] Darüber hinaus verwendet der Cloud-Dienst Oracle Virtual Private (VPD), um eine vollständige Datenisolation auch auf Datenbankebene zu gewährleisten. Durch die von einem externen Sicherheitsunternehmen durchgeführten Penetrationstests wird bestätigt, dass alle Isolationen und Segregationen vorhanden sind.

10.1.7 ID- und Rechtemanagement

[redacted]

- Die Beantragung einer Zugangsberechtigung durchläuft ein gründliches Prüfungs- und Genehmigungsverfahren unter Beurteilung von Risiko, Schweregrad und Auswirkungen.
- Das Verfahren zur Einräumung bzw. Rücknahme von Berechtigungen, die auf den Grundsätzen der „Mindestberechtigung“ und des „begründeten Informationsbedarfs“ beruhen, erfolgt regelmäßig und wird vom Sicherheitsbeauftragten von Ex Libris mindestens einmal jährlich überprüft.
- Nach Genehmigung eines Zugangs bzw. einer bestimmten Tätigkeit gewährt das Zugangskontrollsystem den Zugang zum Server für die bestimmte Tätigkeit und für einen bestimmten Zeitraum auf der Grundlage der beantragten Änderungsaktivität.



Einsatz einer starken Authentisierung (Zwei-Faktor-Authentisierung) für Administratoren und Vier-Augen-Prinzip für kritische Administrationsaufgaben

Der Zugang zur Infrastruktur ist auf der Grundlage von Aufgaben und Zuständigkeiten begrenzt und steht ausschließlich dem Betriebs- und Fachpersonal für die Betreuung und Unterstützung der Kunden zur Verfügung. Ex Libris verfügt sowohl für den Betrieb als auch die Wartung der Systeme und Accounts über strenge Sicherheitsrichtlinien und -verfahren für die Zugangskontrolle sowie die Einrichtung und Löschung von Accounts, einschließlich eines Änderungsmanagementsystems und damit verbundener Abläufe, die auf den Grundsätzen der „Mindestberechtigung" und des „Begründeten Informationsbedarfs" beruhen.

Jegliche Tätigkeiten bzw. Änderungen unterliegen einer erforderlichen Genehmigungskette. Der Sicherheitsbeauftragte von Ex Libris führt Prüfungen und Tests durch, um die Funktionstrennung zu validieren. Die von Ex Libris erfolgreich bestandene ISO 27001Zertifizierung beinhaltet jährliche externe Prüfungen, um die Umsetzung aller Sicherheits- und Minderungsmaßnahmen zu validieren.

[redacted]

Die Authentisierungs-Infrastruktur von Alma verwendet Integrationen mit Identitäts-Providersystemen unter Verwendung von Standardprotokollen wie LDAP und SAML2. Die AlmaIntegration wird unter Verwendung eines Alma-Standardkonfigurations-Elementes konfiguriert - dem Integrationsprofil. Unter Verwendung von SAML2 kann mit Microsoft-Diensten, wie z.B. Active Directory Federation Services (ADFS2) und Unified Access Gateway (UAG) kommuniziert werden. Auch Shibboleth wird unterstützt, sofern die Shibboleth-Implementierung des Unternehmens SAML 2.0 verwendet. Alma kann Nutzer entweder unter Verwendung eines föderierten einfachen Sign-On-Authentication-Systems auf der Grundlage des SAML 2.0 Browser SSO-Profils oder unter Verwendung einer nicht-föderierten Authentisierung authentisieren.

10.1.8 Monitoring und Security Incident Management

Ex Libris verfügt über ein 24x7-NOC, welches alle logischen Netzwerkzugriffe auf die Kundendaten und die Verwendung von Informationswerten protokolliert und überwacht und vom Sicherheitsbeauftragten von Ex Libris überprüft wird. Die mehrschichtigen konzeptionellen Architektursysteme des Monitoring von Ex Libris beinhalten Mehrfachsysteme zur Überwachung der Dienste innerhalb und außerhalb des Rechenzentrums, um sicherzustellen, dass die Dienste mit den besten Leistungsindikatoren betrieben werden.

[redacted]

Ex Libris verfügt über eine Informationssicherheitsrichtlinie, die für alle die Cloud-Dienste nutzenden Kunden gleichermaßen gilt. [redacted] Auf Wunsch füllt Ex Libris einmal jährlich einen Sicherheitsfragebogen aus und stellt dem Kunden Informationen zur Beantwortung aller offenen Fragen zur Verfügung.

Ex Libris hat Änderungsmanagement-Abläufe eingerichtet, so dass alle Tätigkeiten protokolliert, dokumentiert, geplant und genehmigt werden. Der Sicherheitsbeauftragte von Ex Libris validiert die angewandten Verfahren und im Rahmen des ISO-Prüfungs- und Zertifizierungsverfahrens wird überprüft, dass alle Sicherheitsmaßnahmen umgesetzt wurden.

10.1.9 Notfallmanagement

Ex Libris verfügt über ein umfassendes Notfallmanagement sowie einen Notfallplan (Business Continuity Plan) für seine Cloud-Dienste (s. Anlage 7). Dieser Plan wird mindestens einmal jährlich getestet. Der Notfallplan ist orientiert am ISO Standard 23001 und enthält u.a. eine Analyse der Notfallrisiken und Präventionsmaßnahmen, Regelungen zur Notfallfeststellung und -klassifizierung, Wiederherstellungsstrategie, regelmäßige, jährliche Überprüfung und Aktualisierung, Notfallplanübungen. Ex Libris hat eine Notfallrichtlinie (s. Anlage 5) und ein eigenes Notfallmanagement-Team.

10.1.10 Portabilität und Interoperabilität

Sofern sich ein Kunde entschließt, die Ex Libris SaaS-Dienste nicht länger zu nutzen, sieht der SaaS-Vertrag von Ex Libris vor, dass seine Daten im branchenüblichen Standardformat zum Download verfügbar sind.

Ex Libris verwendet Standardprotokolle und -schnittstellen, wie z.B. https und RESTful APIs.

10.1.11 Sicherheitsprüfung und -nachweis

Für seine Kunden hat Ex Libris im Knowledge Center eine Sicherheitszone implementiert, die Updates zu potenziellen Sicherheitslücken und anderen Ereignissen, die die Sicherheit gefährden können, bereitstellt. Zusätzlich enthält die Knowledge Base Artikel über SicherheitsBest Practices und empfohlene Sicherheitsimplementierungen für Kunden.

10.1.12 Personelle Anforderungen

Vor der Einstellung neuer Mitarbeiter_innen unterzieht Ex Libris diese einer Sicherheitsüberprüfung. Für Mitarbeiter, die in kritischen Positionen mit direktem Zugang zu Produktionsdaten von Kunden arbeiten, wie Systemadministratoren, werden Hintergrundprüfungen durchgeführt.

Wenn das Beschäftigungsverhältnis eines/r Mitarbeiter_in bzw. die vertragliche Beziehung mit einem Dienstleister endet, gelangt ein Verfahren zur Löschung seines/ihres Systems zur Anwendung.

Ex Libris verfügt über ein Awareness-Programm zur Informationssicherheit sowie seiner Informationssicherheitsrichtlinie, an dem alle Mitarbeiter_innen teilnehmen. Im Rahmen ihres Employee-Lifecycle-Konzeptes führt die Firma Sicherheitsschulungen und -sensibilisierungen für die Einräumung bzw. Sperrung von Berechtigungen auf der Grundlage der „Mindestberechtigung“ und des „begründeten Informationsbedarfs“ durch. Ex Libris hat die ISO 27001:2013-Zertifizierung zur Bestätigung der Schulung des Personals sowie Hintergrundprüfungen der administrativen Mitarbeiter bestanden und in diesem Zusammenhang auch jährliche Prüfungen der jedem Mitarbeiter übertragenen Rechte eingeführt.

10.2 Nachweis der Sicherheitsmaßnamen des Anbieters

Ex Libris ist ISO 27001:2013-zertifiziert und kann nachweisen, dass alle Sicherheitsmaßnahmen umgesetzt wurden. Es bestehen Richtlinien und Verfahren zur Erkennung von Sicherheitsvorfällen und Einleitung entsprechender Maßnahmen.

Ex Libris beschäftigt einen Sicherheitsbeauftragten, der für die Entwicklung und Umsetzung von Sicherheitsrichtlinien und -maßnahmen zuständig ist. [redacted] Der Sicherheitsbeauftragte verfügt über entsprechende Kenntnisse im Bereich Informationssicherheit sowie die notwendigen Fähigkeiten und Erfahrungen, um die ihm übertragenen Aufgaben in effizienter Weise zu erfüllen.

Der Sicherheitsbeauftragte ist zuständig für die Durchführung von Sicherheitsrisikobewertungen durch unabhängige Dritte (mindestens einmal jährlich) und hält vierteljährlich ein Sicherheitsforum zwecks Bekanntgabe sicherheitsrelevanter Informationen und Sensibilisierung für Schwachstellen ab.

Seit Mai 2016 ist Ex Libris ISO/IEC 27018:2014-zertifiziert. Dieser internationale, kürzlich von der International Organization for Standardization (ISO) veröffentlichte Standard enthält Richtlinien zum Schutz personenbezogener Daten (Personally Identifiable Information, PII) in Cloud-Services. Der ISO/IEC 27018-Standard schreibt allgemein akzeptierte Kontrollziele, Steuerelemente und Leitlinien fest, um sicherzustellen, das PII-Daten ausreichend geschützt sind, wenn die Daten von einem Cloud-Dienstleister verarbeitet werden, und bietet ein gemeinsames Compliance Framework für Cloud-Service-Provider, die sich in einem multinationalen Markt bewegen. Während des Zertifizierungsprozesses hat Ex Libris gezeigt, dass die Ex Libris Cloud-Umgebung persönliche Daten im Einklang mit Datenschutzgesetzen schützt, dass Kunden die volle Kontrolle über ihre Daten behalten, dass Kundendaten nicht für nicht-autorisierte Zwecke genutzt werden und dass das Unternehmen transparent aufzeigt, wo Kundendaten gespeichert und wie sie verarbeitet werden.

10.3 Maßnahmen zur Sicherung der Transparenz

Ex Libris informiert seine Kunden unverzüglich, sofern ein unbefugter Zugriff auf ein Kundendaten speicherndes System erfolgt oder der Verdacht eines Datenschutzverstoßes besteht.

[redacted]

Der Kunde ist berechtigt, die Einhaltung der Datenschutzvorschriften sowie der im Rahmen des Auftragsverhältnisses vertraglich geschlossenen Vereinbarungen im notwendigen Umfang zu überwachen, bzw. durch eine von ihm bevollmächtigte Person überwachen zu lassen, insbesondere durch Beschaffung von Informationen über und Einsichtnahme in die gespeicherten Daten und die datenverarbeitende Software. Das Unternehmen unterstützt eine solche Überwachung.

[redacted]

10.4 Netzwerkverschlüsselung

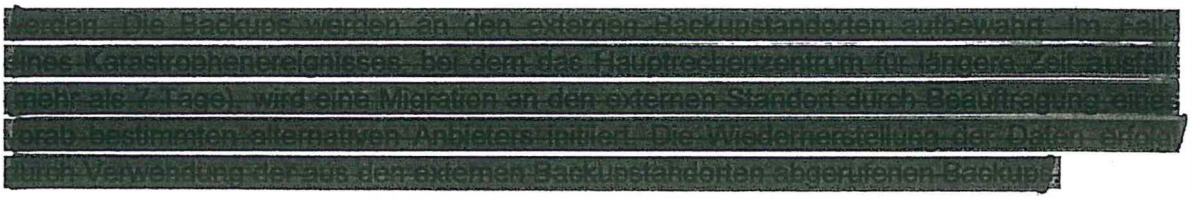
[redacted]

Für die Kunden sind öffentliche SSL-Zertifikate verfügbar.

10.5 Daten-Backup

Ex Libris verfügt über einen hochentwickelten Backup-Plan, der mehrere Snapshots pro Tag, einschließlich eines vollständigen täglichen Backups vorsieht (s. Anlage 7). Die Backups erfolgen auf einen separaten Satz Disk – ein zuverlässiges Backup-Medium, das an einem externen gesicherten Standort aufbewahrt wird. Hierdurch ist gewährleistet, dass im Falle eines lokalen Notfalls Ex Libris jederzeit über eine Kopie der Daten in einem externen und sicheren Disk-Backup verfügt. Ex Libris führt regelmäßig Systembackups zur Sicherung von Anwendungsdateien, Datenbankdateien und Speicherdateien durch. Die im Unternehmen geltenden Datenschutz-richtlinien gelten auch für alle Backup-Dateien. Alle Backup-Dateien unterliegen den Datenschutzrichtlinien von Ex Libris. Die Aufbewahrungsrichtlinie von Ex Libris sieht eine Aufbewahrung von 10 Wochen vor. Die Wiederherstellungsverfahren werden laufend getestet, um im Falle eines Datenverlustes eine rasche Wiederherstellung zu gewährleisten.

[redacted]



Die Wiederherstellungsverfahren werden laufend monatlich getestet, um im Falle eines Datenverlustes eine rasche Wiederherstellung zu gewährleisten. Darüber hinaus wird eine vollständige Kopie der Daten an einem externen gesicherten Standort aufbewahrt.

III. Darstellung Universität

11. Schutzmaßnahmen „auf der letzten Meile“

11.1 Verbindung zum Dienstleister

Die Verbindung zum Dienstleister erfolgt über das Internet mit verschlüsselter https-Verbindung (vgl. Kap. 10.4)

11.2 Maßnahmen zur Absicherung der Endgeräte

Alle PCs der Bibliotheken sind in Windows-Domänen integriert. Eine Nutzung der PCs ohne Anmeldung ist nicht möglich. In einigen Bibliotheken wird an den Ausleih-Theken pro Bereichs- bzw. Zweigbibliothek ein allgemeiner Windows-Account für den Zugang zum PC genutzt.

Nach 15 Minuten Inaktivität am PC wird der Bildschirmschoner aktiviert, der nur mit Eingabe des Passwortes wieder deaktiviert werden kann. Damit sind alle PCs der Bibliotheken weitgehend vor Missbrauch geschützt.

Die Mitarbeiter_innen sind angehalten, sowohl zur Sicherung ihrer persönlichen Gegenstände, als auch zum Schutz des Bibliotheks-Eigentums allgemein (und damit auch der PCs) ihre Arbeitsräume zu verschließen, wenn sich niemand im Raum aufhält.

PCs der Bibliotheken, die in öffentlichen Bereichen aufgestellt sind, sind entweder gesichert (Schloss) oder verdeckt aufgestellt (zum Teil in verschlossenen Schränken). Durch die allgemeine Aufsicht (bzw. durch den Wachschutz) wird gesichert, dass nur bekannte Mitarbeiter_innen PC-Technik aus einer Bibliothek entfernen können.

Auf allen PCs laufen Virenscanner, die laufend aktualisiert werden. Die Mitarbeiter_innen haben keine administrativen Rechte am PC und können keine Programme installieren. So wird die Möglichkeit, Schadprogramme (Viren, Trojaner oder Tastaturlogger) zu installieren auf den PCs sehr erschwert.

➢ Weiteres in Anlage 1 – jeweiliger universitätsspezifischer Teil