Anlage 7

# Notfallplan
# (Business Continuity Plan – BCP)
# für die Cloud-Dienste
# der Ex Libris Group

## VERTRAULICH

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

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

## HAFTUNGSAUSSCHLUSS

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

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

## MARKEN

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

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

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

Oracle ist eine eingetragene Marke der Oracle Corporation.

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

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

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

Google ist eine eingetragene Marke von Google, Inc.

Webadresse: http://www.exlibrisgroup.com

# Inhalt

## Protokollierung von Änderungen

| Art der Information | Dokumentdaten |
|---|---|
| Dokumentname: | Notfallplan (BCP) für die Cloud-Dienste der Ex Libris Group |
| Dokumentverantwortlicher: | Eyal Alkalay – Ex Libris Cloud Engineering Director |
| Genehmigt von: | Yair Amsterdam – Ex Libris Chief Operating Officer |
| Herausgegeben: | 18. April 2011 |
| Geprüft und überarbeitet: | 28. April 2015 |

## Verteilung und Prüfung des Dokumentes

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

# 1) Notfallplan – Überblick

Der Notfallplan für die Cloud-Dienste der Ex Libris Group stellt einen umfassenden Katalog von Maßnahmen dar, die vor, während und nach einem Notfall erforderlich sind. Der Plan wurde entwickelt, um das Risiko auf ein akzeptables Niveau zu begrenzen, indem die zeitnahe Wiederherstellung der entscheidenden Funktionen und Dienste sowie die Wiederherstellung der wesentlichen Produktion innerhalb eines längeren, jedoch zulässigen Zeitrahmens gewährleistet werden. Dieser Plan identifiziert die entscheidenden Aufgaben und Leistungen für die Cloud-Dienste von Ex Libris sowie die hierfür notwendigen Ressourcen. Der Plan sieht Richtlinien und Empfehlungen vor, um sicherzustellen, dass ausreichend Personal und Ressourcen für die Vorkehrungen, Bewertung und Bewältigung von Notfällen zur Verfügung stehen, um eine kurzfristige Wiederherstellung der Dienste zu ermöglichen.

## 1.1 Definitionen

**Notfallplan (Business Continuity Plan – BCP)** – Eine Beschreibung der Vorkehrungen, Ressourcen und ausreichenden Maßnahmen, die es einem Unternehmen ermöglichen, auf einen Notfall zu reagieren und die wesentlichen Betriebsabläufe innerhalb eines vorab definierten Zeitrahmens ohne inakzeptable betriebliche Auswirkungen wieder aufzunehmen.

**Wiederherstellungsplan (Disaster Recovery Plan – DRP)** – ein technisches Dokument, welches die Prozesse, Richtlinien und Abläufe im Hinblick auf die Implementierung von Vorsorgemaßnahmen sowie die Notfallvorbereitung und die Aufrechterhaltung bzw. Wiederherstellung der Leistungen im Katastrophenfall beschreibt.

**Notfall** – ein plötzliches, ungeplantes und verhängnisvolles Ereignis, welches einen vollständigen Ausfall bzw. eine signifikante Unterbrechung der für den Kunden relevanten Dienste verursacht. Primäres Ziel des Plans ist es, das Risiko geringfügiger Notfälle sowie die Auswirkungen erheblicher Notfälle zu mindern.

## 1.2 Ziele des Notfallplans

Vorrangiges Ziel der Notfallplanung ist die Erstellung, Erprobung und Dokumentierung eines gut strukturierten und leicht verständlichen Plans zur Unterstützung einer schnellstmöglichen und wirksamen Wiederherstellung der Ex Libris Cloud-Dienste nach einem unvorhergesehenen Katastrophen- bzw. Notfallereignis, durch welches die Cloud-Dienste und der Geschäftsbetrieb von Ex Libris unterbrochen wurden.

Mit diesem Dokument sind folgende Ziele verbunden:

- Entwicklung einer Notfallplanstruktur zur Bewältigung von Notfällen, welche die Cloud-Dienste von Ex Libris beeinträchtigen.
- Dokumentierung der für die Umsetzung des Notfallplans entscheidenden Informationen und Abläufe.
- Vorlage eines Maßnahmenkatalogs zur Wiederherstellung wichtiger Cloud-Dienste innerhalb einer Mindestanzahl von Tagen nach Aktivierung des Plans

- Festlegung von Richtlinien mit einem Eskalationsplan für eine Notfallklassifizierung, die zur Anwendung dieses Notfallplans führt.
- Beschreibung einer Organisationsstruktur zur Durchführung des Plans und Sicherstellung, dass alle Mitarbeiter ihre Aufgaben bei der Implementierung eines solchen Plans vollständig verstehen.
- Gewährleistung einer ordnungsgemäßen Wiederherstellung nach einem Notfall, Minimierung des Risikos des Produktions- bzw. Leistungsausfalls

## 1.3 Notfallrichtlinie

Die Geschäftsleitung von Ex Libris hat die folgenden Richtlinien beschlossen:

- Das Unternehmen entwickelt einen umfassenden Notfallplan.
- Es wird eine formelle Risikobewertung vorgenommen, um die Anforderungen für den Notfallplan zu ermitteln.
- Der Notfallplan muss alle wesentlichen und kritischen Infrastrukturelemente, Systeme und Dienste sowie die wesentlichen Geschäftstätigkeiten abdecken.
- Der Notfallplan ist regelmäßig zu testen, um sicherzustellen, dass er in Notfallsituationen zur Anwendung gelangt und dass Management und Mitarbeiter die Durchführung des Plans verstehen.
- Alle Mitarbeiter der Ex Libris Cloud-Dienste müssen den Notfallplan und ihre jeweiligen eigenen Aufgaben kennen.
- Der Notfallplan ist regelmäßig zu aktualisieren, um veränderte Umstände zu berücksichtigen.

## 1.4 Plangrundlagen

Der Notfallplan wurde auf Grundlage der folgenden Annahmen entwickelt:

- Dieses Dokument beinhaltet eine Planung für den größtmöglichen Notfall. Sofern jedoch ein Ausfall des Dienstes in geringerem Ausmaß auftritt, ist ein solcher Vorfall von diesem Plan umfasst.
- Die Ursache des Notfalls wird für eines der Rechenzentren von Ex Libris lokalisiert (Chicago, Amsterdam oder Singapur).
- Der Cloud-Dienst von Ex Libris ist durch eine Colocation-Vereinbarung mit einem führenden Anbieter von Rechenzentren (Equinix) verbunden. Der Rechenzentrums-Provider sorgt für die Grund-Infrastruktur, die bei einem Notfall benötigt wird.

## 1.5 Aufgaben und Beschreibung der Notfallteams

- **Notfallmanagement-Team** – Zuständig für die Gesamtleitung sowie die notwendigen Entscheidungen und Beschlüsse zur Umsetzung des Notfallplans. Das Team besteht aus dem Ex Libris Chief Operating Officer (COO) sowie den Direktoren der Cloud-Dienste, denen die Leitung innerhalb ihrer entsprechenden Bereiche obliegt.

- **Notfallplan-Koordinator (BCC)** – Ein Mitglied des Notfallmanagement-Teams, zuständig für die Entwicklung, Koordinierung, Schulung, Eignungsprüfung und Implementierung des Notfallplans.

- **Teamleiter des Notfall-Teams** – Zuständig für die Durchführung der Aufgaben und Bestimmungen des Notfallplans, einschließlich der Zuweisung von Aufgaben an die Mitarbeiter, Einholung externer Datenbackups, Kontakte zu den Herstellern, Überwachung der Arbeitsfortschritte und Statusmeldungen an das Notfallteam. Das Team besteht aus allen Teamleitern und Managern der Ex Libris Cloud-Dienste.

- **Notfallzentrum (Emergency Operations Center – EOC)** – Eine vom Notfallmanagement-Team eingerichtete zentrale Koordinierungsstelle für die Dauer der Wiederherstellungsarbeiten. Dieser Standort wird normalerweise am Hauptsitz der Ex Libris Group eingerichtet.

# 2) Notfallrisiken und Prävention

So wichtig ein Notfallplan auch ist – Maßnahmen zur Verhinderung bzw. Minderung der Auswirkungen von Notfällen im Voraus sind von noch größerer Bedeutung. Dieser Teil des Plans prüft die unterschiedlichen Bedrohungen, die zu einem Notfall führen können, sowie die Maßnahmen, die wir zur Minimierung unseres Risikos ergreifen sollten. Bei einem Katastrophenereignis können viele unterschiedliche Ausfälle auftreten. Nachstehend sind einige Ereignisse und Situationen aufgeführt, die bei der Erstellung des Plans berücksichtigt werden.

## 2.1 Präventivmaßnahmen

| Möglicher Notfall | Präventivmaßnahmen |
|---|---|
| **Geräte-/Hardwareausfall** | • **Redundante Infrastruktur** – Dies wird durch die Architektur und Designstandards von Ex Libris auf allen Infrastrukturebenen gewährleistet, einschließlich mehrfacher Firewalls, Switches, Speichercontrollern, Load Balancers (Lastverteilern), kontrollierbare PDUs, Verkabelung, Stromquellen und Standby-Hardware.<br>• **Erstklassige Hardwaresupport-Verträge mit kurzen SLAs für die Reparatur bzw. den Austausch von Hardware der Cloud-Infrastruktur** – Das Ergebnis ist ein geringerer Zeitaufwand für den Austausch ausgefallener Server, Festplatten-Arrays und Netzwerkgeräte.<br>• **Providerunabhängige Internetverbindungen** – Dies wird durch die Netzwerkarchitektur und Implementierungsstandards von Ex Libris, zusammen mit den die Anforderungen unterstützenden Leistungen des Rechenzentrums-Providers gewährleistet. |
| **System- und Softwareausfall** (Datenunterbrechung, Programmierfehler) | • **Datenbackups** – Auf allen Ebenen, einschließlich Plattform, Anwendung und Kundendaten<br>• **24/7 Anwendungssupport und technischer Support –** Dies ist durch den 24/7 HUB (NOC) der Ex Libris Group gewährleistet.<br>• **Verwendung von Disk Protection Shared Storage-Technologie** auf Plattform- und Anwendungsebene |

| | |
|---|---|
| **Stromausfall** | • **Unterbrechungsfreie Stromversorgung (USV) und Backupgeneratoren zur Aufrechterhaltung der Systeme im Falle eines Stromausfalls** – Die Rechenzentren sind vollständig mit einer unterbrechungsfreien Stromversorgung, Backupsystemen und einer Redundanz von N+1 (oder höher) ausgestattet. Dieser Service erfolgt durch den Rechenzentrums-Provider.<br>• **Redundante Stromversorgung, Kühlung** – Eine wirksame und effiziente Klimatisierungsinfrastruktur, die eine ausreichende Widerstandsfähigkeit für hochkomplexe Hochverfügbarkeitsumgebungen bietet. Dies wird durch die Netzwerkarchitektur und Implementierungsstandards von Ex Libris, zusammen mit den die Anforderungen unterstützenden Leistungen des Rechenzentrums-Providers gewährleistet.<br>• **Überspannungsschutz zur Minderung der Auswirkungen von Überspannungen auf elektronische Geräte** – Dies wird durch den Rechenzentrums-Provider durch Implementierung sowohl entsprechender Schutzvorrichtungen für die Anlage insgesamt als auch Überspannungsschutzsteckdosen in den Racks gewährleistet. |
| **Mut- und böswillige Handlungen** (Sicherheitsverstöße, Denial-of-Service-Angriffe, Sabotage, Terrorakte) | • **Physische Zugangssicherheit** – 24/7-Sicherheit, biometrische Authentifizierung, Videoüberwachung, befugtes Personal.<br>• **Infrastruktursicherheit** – Verstärkung, Änderungsmanagementverfahren, Risikobewertung, Patch Management, Passwortrichtlinie, Prüfung und Auswertung durch Security Officer.<br>• **Netzwerksicherheit** – Trennung, Schwachstellenscans, Intrusion Prevention System (IPS), TLS/SSL-verschlüsselte Kommunikation.<br>• **Anwendungssicherheit** – Security Development Lifecycle (Sicherheitsentwicklungszyklus – SDL), Penetrationstests, Schwachstellenanalyse, OWASP Top10, Prüfung und Auswertung durch Security Officer.<br>• **Datensicherheit** – Datenisolierung, Verschlüsselung, Trennung, Medienbereinigung (DoD 5220.22-M).<br>• **Identitäts- und Zugangskontrolle** – SSO, S/LDAP, SAML/Shibboleth, Rollenbasierte Zugangskontrolle (RBAC).<br>• **Monitoring & Notfallmanagement** – 24x7-Monitoring, Chief Security Officer (CSO), Meldung von Sicherheitsverstößen.<br>• **Personal** – Security Awareness-Schulungen, Geheimhaltungsvereinbarungen, Einhaltung von Vorschriften<br>• **Compliance & Audit** – ISO 27001, SSAE-16, EU Safe Harbor, Datenverarbeitungsverträge, unabhängige Prüfung. |

| | |
|---|---|
| **Naturkatastrophen**<br>(Erdbeben, Hochwasser, Stürme, Tornados, Hurrikane, Brände) | • **Brandschutz** – VESDA (Very Early Smoke Detection Apparatus) zur Frühwarnung installiert; analog adressierbare Brandmelder auf 3 Ebenen installiert; automatischer Hochdruck-HI-FOG-Systemalarm, CO2-Feuerlöscher und Brandunterdrückungssysteme werden vom Rechenzentrums-Provider gestellt.<br>• **24/7-Support am Standort des Rechenzentrums** – Das Betriebspersonal ist 24/7 vor Ort und gemeinsam mit dem Sicherheitspersonal vollständig in der Brandbekämpfung (Handfeuerlöscher) geschult, wobei ein strenger Maßnahmenkatalog im Hinblick auf das Verhalten bei Notfällen, einschließlich einer Evakuierung, gilt. Zuständig ist der Rechenzentrums-Provider, Smart Hands Services.<br>• **Überschwemmungen** – Die Überschwemmungsproblematik wird während der Standortsuche und der Standorterrichtung anhand der FEMA-Maps (bzw. vergleichbarer Dokumentation) und hochwassergefährdeten Gebiete überprüft. Zuständig ist der Rechenzentrums-Provider, Smart Hands Services.<br>• **Erdbeben** – Die Bauvorschriften berücksichtigen die geographische Lage, die Bodenbeschaffenheit für das Fundament sowie die Funktion des Gebäudes (Rechenzentren gehören der Belegungsstufe III an) und weisen sodann die Seismischen Design-Kategorien (A-F) zu, auf deren Grundlage die Bauingenieure ihre Berechnungen stützen. Zuständig ist der Rechenzentrums-Provider, Smart Hands Services. |

## 2.2 Redundanzstrategien

Die folgenden Redundanzstrategien sind in der Umgebung der Cloud-Dienste der Ex Libris Group verfügbar:

- **Active/Active Load Balancing** – Der Datenverkehr wichtiger Server wird gleichmäßig zwischen zwei oder mehr Servern aufgeteilt. Bei Ausfall eines der Server wird der Datenverkehr automatisch und reibungslos auf den arbeitenden Server übertragen.
- **Active/Active Virenschutz** – Der Datenverkehr wird zwischen zwei oder mehr Virenschutzscangeräten zwecks Lastverteilung aufgeteilt. Der Datenverkehr wird automatisch und reibungslos auf den arbeitenden Server übertragen.
- **Aktives/Passives Netzwerk** – Das externe Netzwerk stammt aus einer primären zweckbestimmten Verbindung mit automatischem Failover in eine sekundäre zweckbestimmte Verbindung. Das interne Netzwerk ist auf allen Ebenen redundant.
- **Active/Passive Multiply ISP-Provider** – Multi-ISP-Verbindung zum Hauptstandort unter Verwendung eines Managed Internet Route Optimizers mit automatischem Failover.
- **Active/Passive Firewall** – Der Netzwerkverkehr nutzt eine primäre Firewall mit automatischem Failover zu einer sekundären Firewall.

- **Active/Active Storage** – Die Daten werden zwischen zwei oder mehr Storage Controllern zwecks Lastverteilung und Übernahme bei einem Ausfall verteilt.

- **Verfügbare On-site Serverkapazität** – Auch als „Onsite Cold Equipment" bezeichnet. Für den Fall eines katastrophalen Hardwareausfalls, der nicht kurzfristig behoben werden kann, wird die virtuelle Instanz der Hosting-Umgebung des Kunden von einem vorhandenen Standby-Server installiert, auf welchen vorab das entsprechende OS und die administrativen Anwendungen geladen wurden. Bei Bedarf kann dann eine Wiederherstellung der Daten des Kunden aus dem Onsite- bzw. den Offsite-Backups erfolgen.

## 2.3 Backup-Strategien

Ex Libris verfügt über einen hochentwickelten Backup-Plan, der mehrere Snapshots pro Tag, einschließlich eines vollständigen täglichen Backups vorsieht. Die Backups erfolgen auf einen separaten Satz Disks – ein zuverlässigeres und schnell verfügbares Backup-Medium, das sowohl vor Ort, als auch an einem externen gesicherten Standort über eine private, zweckbestimmte und schnelle sichere Verbindung aufbewahrt wird. Hierdurch ist gewährleistet, dass im Falle eines lokalen Notfalls Ex Libris jederzeit über eine Kopie der Daten vor Ort und 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 Datenschutzrichtlinien gelten auch für alle Backup-Dateien. Alle Backup-Dateien unterliegen den Datenschutzrichtlinien von Ex Libris. Die Wiederherstellungsverfahren werden laufend getestet, um im Falle eines Datenverlustes eine rasche Wiederherstellung zu gewährleisten.

- **Backup vor Ort** – Vollständige Backups für OS-Plattform, Anwendung und Kundendaten erfolgen mindestens täglich (mehrere Snapshots während des Tages für kritische Dienste/Systeme) unter Verwendung einer Speicher-Snapshot-Technologie. Die Backups werden eine Woche lang vor Ort auf einem separaten Satz von Disks aufbewahrt. Die Snapshots werden automatisch mit spezifischen, vom Betriebssystem erkannten Zugangsbeschränkungswerten in einen speziellen Verzeichnissatz übertragen, wodurch jederzeit eine leichte und unverzügliche Wiederherstellung durch befugte Mitarbeiter von Ex Libris ermöglicht wird.

- **Offsite-Backup** – Vollständige Backups für OS-Plattform, Anwendung und Kundendaten erfolgen täglich unter Verwendung einer Snap Mirror-Technologie über eine private, dedizierte, schnelle und sichere Netzwerkverbindung aus dem Hauptrechenzentrum an einen externen Backupstandort unter Verwendung derselben Speichertechnologie wie jener am Hauptstandort. Entsprechend den Datenschutzrichtlinien von Ex Libris werden die externen Backupstandorte im selben Gebiet (NA, EMEA und APAC) wie die Hauptstandorte – mit ausreichender und geeigneter physischer Distanz zueinander – betrieben. Die Backups können rund um die Uhr von autorisierten Mitarbeitern von Ex Libris für das Hauptrechenzentrum abgerufen werden. Die Backups werden an den externen Backupstandorten aufbewahrt.

# 3) Notfallfeststellung und -klassifizierung

Die Feststellung eines Ereignisses, das zu einem die Cloud-Dienste von Ex Libris beeinträchtigenden Notfall führen könnte, liegt in der Verantwortung des Ex Libris 24x7 HUBs bzw. jenes/jener Angehörigen der Ex Libris Cloud Group, der/die eine sich anbahnende Notfallsituation in einem der Funktionsbereiche des Cloud-Dienstes zuerst feststellt bzw. hiervon Kenntnis erlangt.

## 3.1 Notfallmeldung

Wer auch immer den Notfall feststellt, muss den Ex Libris Cloud Operations Director bzw. den Ex Libris Cloud Engineering Director benachrichtigen. Über eine gewisse Fehlertoleranz bei der ersten Reaktion hinaus, ermöglicht diese Aufgabenteilung ein effektives Arbeiten in Schichten während des Wiederherstellungsprozesses.

Der Ex Libris Cloud Operations Director bzw. der Ex Libris Cloud Engineering Director richtet das Notfallzentrum (EOC) ein, überwacht die weitere Entwicklung und benachrichtigt gegebenenfalls das Notfallmanagement-Team. Die vollständige Liste der Notfallkontakte für die Cloud-Dienste von Ex Libris ist in Anlage A beigefügt.

Üblicherweise geht der erste Alarm beim Network Operation Center (NOC) des Rechenzentrums-Providers und/oder den örtlichen Ordnungskräften über die entsprechenden Überwachungssysteme ein. Sofern durch den Notfall ein übliches Alarmsystem nicht aktiviert wird, sind diese beiden Parteien unverzüglich durch den Ex Libris Cloud Operations Director bzw. den Ex Libris Cloud Engineering Director zu benachrichtigen.

## 3.2 Ermittlung des Personalstatus

Eine der ersten Aufgaben des Ex Libris Cloud Operations Director bzw. des Ex Libris Cloud Engineering Directors ist es, den Personalstatus zum Zeitpunkt des Notfalleintritts zu ermitteln. Das Sicherheitspersonal vor Ort wird nach Eintritt des Notfalls alle notwendigen Rettungs- und Erste Hilfe-Maßnahmen für die von dem Notfallereignis betroffenen Personen einleiten. Der Director sollte jedoch eine Liste der körperlich unversehrten Personen erstellen, die für eine Unterstützung des Wiederherstellungsprozesses zur Verfügung stehen. Die Versorgung von Menschen ist eine äußerst wichtige Aufgabe und muss daher unmittelbar nach Eintritt des Notfalls oberste Priorität haben. Während mit der Wiederherstellung des Computer- und Netzwerkbetriebes eine riesige technische Aufgabe vor uns liegt, dürfen wir die auf dem Spiel stehenden menschlichen Interessen nicht aus dem Blick verlieren.

## 3.3 Schadensermittlung

Um ermitteln zu können, in welcher Weise der Notfallplan nach einer schwerwiegenden Unterbrechung des Dienstes umgesetzt wird, ist es wichtig, die Art und das Ausmaß der Schäden am System zu bewerten.

Nachdem die entsprechenden Ansprechpartner des Rechenzentrums-Providers benachrichtigt wurden, werden die Teamleiter des Notfallteams kontaktiert, damit eine vorläufige Einschätzung erfolgen kann, ob eine Schadensermittlung vor Ort erforderlich bzw. durchführbar ist.

Die Schadensermittlung dient der unter den gegebenen Umständen schnellstmöglichen Feststellung des Ausmaßes der Schäden an für den Betrieb entscheidenden Computeranlagen und dem entsprechenden Rechenzentrum, wobei die Sicherheit des Personals oberste Priorität bleibt.

Hierbei sind folgende Aspekte zu berücksichtigen:

- Ursache des Notfalls bzw. der Unterbrechung
- Möglichkeit weiterer Unterbrechungen bzw. Schäden
- Betroffener Bereich
- Status der physischen Infrastruktur (z.B. strukturelle Integrität des Rechenzentrums, Zustand der Stromversorgung, Telekommunikations- sowie Heizungs- und Lüftungs-/Umweltbedingungen)
- Bestandsaufnahme und Funktionszustand der Ex Libris-Geräte
- Art der Schäden an Geräten oder Daten (z.B. Wasser, Feuer, physische Auswirkungen, Überspannung)
- Geschätzte Zeit zur Wiederherstellung des normalen Betriebs

## 3.4 Notfall-Klassifizierung

Vorrangiges Ziel der Schadensermittlung ist die Bestimmung der Schwere des Notfalls und Einschätzung der benötigten Zeit zur Wiederherstellung der Ex Libris Cloud-Dienste in einen Normalbetrieb.

Die Ex Libris Cloud Services Group hat Notfälle und Notfallereignisse in die folgenden drei Kategorien eingeteilt – geringfügig, erheblich und Katastrophenereignis:

- **Geringfügiger Notfall** – Ein geringfügiger Notfall ist durch eine erwartete Ausfallzeit von **höchstens 48 Stunden gekennzeichnet.** Es können Schäden an Hardware, Software und/oder der Betriebsumgebung vorhanden sein. Die Ex Libris Cloud-Dienste können am Hauptstandort in einen normalen Betrieb zurückgeführt werden und Reparaturen können schnellstmöglich begonnen werden:
- **Erheblicher Notfall** – Ein erheblicher Notfall ist durch eine erwartete Ausfallzeit von mehr als **48 Stunden, jedoch weniger als 7 Tagen** gekennzeichnet. Bei einem erheblichen Notfall bestehen normalerweise weitreichende Schäden an Systemhardware, Software, Netzwerken und/oder Betriebsumgebung. Die Ex Libris Cloud-Dienste können mit Hilfe bestimmter Wiederherstellungsteams in einen Normalbetrieb zurückgeführt werden, die unmittelbar mit der Wiederherstellung des Normalbetriebs am Hauptstandort beauftragt werden.
- **Katastrophenereignis** – Ein Katastrophenereignis ist durch eine erwartete **Ausfallzeit von mehr als 7 Tagen** gekennzeichnet. Das Rechenzentrum ist in dem Ausmaß zerstört, dass ein alternativer Standort genutzt werden muss. Die Schäden an der Systemhardware, Software und/oder der Betriebsumgebung erfordern den vollständigen Austausch/die vollständige Erneuerung aller betroffenen Systeme. Es ist die Umsetzung des Wiederherstellungsplans an einem externen Standort erforderlich, um den Cloud-Dienst von Ex Libris in einen Normalbetrieb zurückzuführen.

# 4) Wiederherstellungsstrategie

## 4.1 Wiederherstellungsstrategien (DR-Strategien) für Geringfügige und Erhebliche Notfälle

### 4.1.1 Datenverlust durch Hardware- bzw. Softwareausfall

In diesem Abschnitt werden die Maßnahmen zur Wiederherstellung von Datenverlusten bzw. Unterbrechungen aufgrund eines geringfügigen bzw. erheblichen Notfalls auf **Hardware- und Softwareebene** erläutert.

**Ursachenanalyse**

- Es erfolgt ein Troubleshooting durch einen Techniker des DR-Teams zur Ermittlung der unmittelbaren Ursache des Datenverlustes.
- Sofern der Verlust auf einen Hardwareausfall zurückzuführen ist, wird das DR Hardware Response Team benachrichtigt.
- Sofern der Verlust auf einen Softwareausfall bzw. auf menschliches Versagen zurückzuführen ist, wird das DR Application Response Team benachrichtigt.

**Datenverlust durch Hardwareausfall**

- Die virtuelle Instanz der Hosting-Umgebung des Kunden wird von vorhandener Standby-Hardware installiert, auf welche vorab das entsprechende Betriebssystem und die administrativen Anwendungen geladen wurden.
- Der Systemhersteller wird kontaktiert und um einen Notfallservice gebeten.
- Sofern erforderlich, erfolgt eine Wiederherstellung der Daten aus einem Onsite- bzw. Offsite-Backup.
- Die Reparatur bzw. der Austausch der Hardware wird durchgeführt.
- Die Kundeninformation im Ex Libris Statusportal (status.exlibrisgroup.com) wird aktualisiert.

**Datenverlust aufgrund von Datenunterbrechung bzw.**

**Anwendungsproblemen**

- Es erfolgt eine Reparatur bzw. Neuinstallation der Software.
- Die Wiederherstellung der Daten erfolgt aus einem Onsite- bzw. Offsite-Backup.
- Die Kundeninformation im Ex Libris Statusportal (status.exlibrisgroup.com) wird aktualisiert.

### 4.1.2 Unterbrechung des Dienstes aufgrund von Hardwareproblemen bzw. Ereignissen im Rechenzentrum

Nachstehend sind die Maßnahmen zur Wiederherstellung der Cloud-Dienste im Fall eines geringfügigen bzw. erheblichen Notfalls auf Hardware- bzw. Rechenzentrumsebene erläutert.

**Ursachenanalyse**

- Ein Techniker des DR-Teams führt eine Problemerkennung durch, um die unmittelbare Ursache der Unterbrechung bzw. des Ausfalls des Dienstes zu ermitteln.
- Sofern der Verlust auf einen Hardwareausfall zurückzuführen ist, wird das DR Hardware Response Team bzw. das DR Operations Team des Rechenzentrums-Providers benachrichtigt.
- Sofern der Verlust auf einen Softwareausfall bzw. auf menschliches Versagen zurückzuführen ist, wird das DR Application Response Team benachrichtigt.

**Unterbrechung des Dienstes aufgrund eines Hardwareausfalls des Rechenzentrums-Providers**

- Die Abhilfemaßnahmen des Rechenzentrums-Providers werden bis zu ihrem Abschluss durch den Ex Libris Techniker verfolgt.
- Die Reparatur bzw. der Austausch der Hardware wird durchgeführt.
- Die Kundeninformation im Ex Libris Statusportal (status.exlibrisgroup.com) wird aktualisiert.

**Unterbrechung des Dienstes aufgrund eines Hardwareausfalls des Ex Libris Cloud-Dienstes**

- Die virtuelle Instanz der Hosting-Umgebung des Kunden wird von vorhandener Standby-Hardware installiert, auf welche vorab das entsprechende OS und die administrativen Anwendungen geladen wurden.
- Der Systemhersteller wird kontaktiert und um einen Notfallservice gebeten.
- Die Reparatur bzw. der Austausch der Hardware wird durchgeführt.
- Sofern erforderlich, werden alle notwendigen Softwarekonfigurationen auf der reparierten bzw. ausgetauschten Hardware ausgeführt.
- Die Kundeninformation im Ex Libris Statusportal (status.exlibrisgroup.com) wird aktualisiert.

## 4.2 Wiederherstellungsstrategie im Fall eines Katastrophenereignisses

Nachstehend sind die Maßnahmen zur Wiederherstellung der Cloud-Dienste im Fall eines Katastrophenereignisses im Rechenzentrum aufgeführt:

- Die Teamleiter des Notfallteams ermitteln gemeinsam mit dem Rechenzentrums-Provider das Ausmaß der Schäden am Rechenzentrum.
- Für den Fall, dass der Hauptstandort für einen längeren Zeitraum (mehr als 7 Tage) ausfällt, wird die Kundeninformation im Ex Libris Statusportal aktualisiert.
- Es wird eine Wirtschaftlichkeitsbewertung hinsichtlich der Bergung von unternehmenseigenen Ex Libris-Geräten aus der betroffenen Anlage durchgeführt.
- Gleichzeitig wird ein vorab bestimmter alternativer Rechenzentrums-Provider benachrichtigt und beauftragt.
- Jegliche Hardware, die gerettet werden kann, wird von Ex Libris für eine Verwendung am festgelegten Wiederherstellungsstandort beansprucht.
- Es werden Beschaffungsmaßnahmen zum Austausch der nicht mehr verwertbaren Geräte eingeleitet.
- Ein Konzept und ein Zeitplan für die Implementierung des Wiederherstellungsstandortes werden ausgearbeitet und den Interessenvertretern der Ex Libris-Kunden übermittelt.
- Der Implementierungsplan wird ausgeführt.
- Die Interessenvertreter von Ex Libris und der Kunden werden von der Wiederaufnahme des Dienstes aus einem alternativen Rechenzentrum unterrichtet.

### Lokalisierung und Verwertung von Daten und Geräten

Erste Bemühungen dienen dem Schutz und der Erhaltung verwertbarer Computer- und Netzwerkausstattung (jegliche Hardware, die gerettet werden kann, wird von Ex Libris zwecks Verwendung am Wiederherstellungsstandort zurückgefordert). Insbesondere werden alle Backup-Speichermedien (Festplatten, Backup-Bänder) identifiziert und entweder vor den Elementen geschützt oder in eine saubere, trockene Umgebung außerhalb des betroffenen Standortes verbracht.

### Bestimmung des Standorts für die Wiederherstellung

Eine Inspektion des Rechenzentrums und der Telekommunikationsschränke erfolgt durch die Teamleiter des Notfallteams, um den für eine Wiederherstellung des betriebsfähigen Zustands verwertbarer Geräte benötigten Zeitaufwand zu ermitteln, sofern angemessene Einrichtungen vorhanden sind, die genutzt werden können. Es wird sodann entschieden, ob ein externer Standort genutzt wird, an welchen die Computer- und Netzwerkausstattung vorübergehend verbracht werden kann, bis der Hauptstandort verfügbar ist. Sofern eine solche Einschätzung ergibt, dass eine Wiederherstellung am ursprünglichen Standort mehr als 7 Tage beansprucht, wird eine Migration an den externen Wiederherstellungsstandort durch Benachrichtigung und Beauftragung eines vorab bestimmten alternativen Rechenzentrums-Providers eingeleitet.

### System- und Datenwiederherstellung

Soweit möglich, werden verwertbare Geräte durch Ex Libris verwendet. Sofern Geräte irreparabel beschädigt sind, arbeitet die Einkaufsabteilung von Ex Libris mit unseren Herstellern (in Anlage B aufgeführt) gemeinsam daran, einen Austausch der Geräte zu beschleunigen.

Die Wiederherstellung der Daten erfolgt unter Verwendung der seitens des betroffenen Standortes von den externen Backupstandorten abgerufenen Backups. Backups können auf unterschiedlichen Medien gespeichert sein, einschließlich Festplatten und Magnetbändern. Nach der Identifizierung verwertbarer Geräte konzentrieren sich die ersten Bemühungen zur Datenwiederherstellung auf die Wiederherstellung des/der Betriebssystems/e für jedes System. Im Anschluss werden wichtige Systemdaten wiederhergestellt. Nach der Wiederherstellung der Systemdaten werden die individuellen Kundendaten wiederhergestellt.

### Rückführung an wiederhergestellte Hauptstandorte

Während des Wiederherstellungsprozesses an einem alternativen externen Standort wurde voraussichtlich mit der physischen Instandsetzung des Hauptrechenzentrums begonnen. Sobald das Rechenzentrum zur Belegung zur Verfügung steht, müssen die am externen Standort aufgebauten Systeme wieder an ihren eigentlichen Standort verbracht werden.

Dieser Abschnitt erläutert die für eine Rückübertragung des Dienstes an den Hauptstandort notwendige logistische Planung für den Fall, dass eine Verlegung des Betriebs an einen Wiederherstellungsstandort zur Minderung eines Katastrophenereignisses erforderlich wurde.

Die Betriebsbereitschaft am ursprünglichen Hauptstandort ist vor Durchführung dieses Schrittes zu verifizieren. Nach entsprechender Verifizierung werden die folgenden Maßnahmen eingeleitet:

- Abstimmung des Migrationsplans mit dem Rechenzentrums-Provider
- Abstimmung des Migrationsplans mit dem Kunden
- Vorbereitung der Cloud-Dienste für die Migration
- Ausführung der Migration
- Systemabnahmetest (Systems Acceptance Test – SAT) und Benutzer-Abnahmetest (User Acceptance Test – UAT)
- Meldung der durchgeführten Migration an die für den Betrieb verantwortlichen Personen

# 5) Regelmäßige Aktualisierung und Übung des Plans

Einen Notfallplan zu haben, ist wichtig. Der Plan wird jedoch schnell hinfällig, wenn nicht auch praktikable Abläufe zur Aktualisierung des Plans entwickelt und implementiert werden. In diesem Abschnitt werden die notwendigen Maßnahmen erläutert, um den Plan aktuell zu halten.

## 5.1 Notfall-Koordinator (BCC)

Dem Notfall-Koordinator obliegt die Gesamtverantwortung für den Entwurf, die Erstellung, die Koordinierung, Implementierung, Verwaltung, Schulung, Awareness-Programme und Aktualisierung des Notfallplans. Der Notfall-Koordinator befolgt die Best Practices der DRI International Professional Practices for Business Continuity Planners (siehe aktuelle Version unter www.drii.org).

Gemäß den DRII Professional Practices hat der Notfall-Koordinator folgende Aufgaben:

- Notfallprojektkoordination und -management.
- Durchführung notwendiger Risikobewertungen und -minderungen.
- Entwicklung der Notfallstrategie(n) und Einholung entsprechender Genehmigungen.
- Erstellung und Implementierung des Notfallplans.
- Entwicklung, Pflege, Koordinierung, Übung und Auswertung des Notfallplans.

## 5.2 Aktualisierung des Notfallplans

Der Plan wird jährlich überprüft und aktualisiert. Alle Teile des Plans werden durch den Ex Libris COO und den Cloud Engineering Director überprüft. Sofern es notwendig ist, dass Teile des Plans geändert werden müssen bzw. durch andere Cloud-Teams neu gefasst oder überprüft werden müssen, beauftragt der COO das entsprechende Team mit diesen Aufgaben. Darüber hinaus wird der Plan regelmäßig einem Eignungstest unterzogen und alle Fehler werden berichtigt. Das Notfallmanagement-Team überwacht die einzelnen Komponenten und Dateien und gewährleistet, dass diese die für den übrigen Plan geltenden Standards erfüllen.

## 5.3 Notfallplanübungen (Eignungsprüfung)

Der Notfall-Koordinator ist zuständig für die Durchführung regelmäßiger Notfallplanübungen unter Einsatz unterschiedlicher Methoden (strukturierte Walkthrough-Übungen, taktische Übungen und technische Übungen für die Teamleiter des Notfallteams) bzw. einer Kombination dieser Methoden. Nach Abschluss der Übung wird dem Notfallmanagement-Team ein Bericht über den Erfolg und/oder Misserfolg der Übung übermittelt. Im Anschluss findet eine Besprechung hinsichtlich möglicher Verbesserungen des Plans statt. Alle Änderungen des Dokumentes aufgrund der Testergebnisse und der Besprechung innerhalb des Managements werden in das Dokument aufgenommen.

# Anlage A: Kontaktdaten BCP- und DR-Team

Die nachstehende Liste enthält die relevanten Angaben zu den Ex Libris Group DR-Projektteamleitern:

| Name | Funktion | Mobil | E-Mail |
|---|---|---|---|
| Ex Libris 24x7 Hub | Ex Libris 24/7 Support und Kommunikation | + *-***-***-*** | ********** |
| ********** | Ex Libris Chief Operating Officer | +*-***-***-**** | ********** |
| ********** | Cloud Engineering Director | +*-***-***-**** | ********** |
| ********** | Cloud Operations Director | +***-**-***-**** | ********** |
| ********** | Security Officer | +***-**-***-**** | ********** |
| ********** | Cloud Infrastructure Engineer | +***-**-***-**** | ********** |
| ********** | Cloud Production Engineer | +***-**-***-**** | ********** |
| Hosting-Rechenzentrum First Touch Response | Rechenzentrum 24/7 Smart Hands, Operations und Support | + *-***-***-*** | ********** |
| ISP, CDN | 24/7 NOC | + *-***-***-*** | ********** |

* Aus Datenschutzgründen verdeckt

# Anlage B: Herstellerkontaktdaten

Nachstehend finden Sie die Kontaktdaten unserer derzeitigen Hauptthersteller der meisten Komponenten dieses Wiederherstellungsplans.
Diese Liste wird für alle Hersteller der Ex Libris Cloud-Dienste im Hinblick auf die Wiederherstellungsbemühungen im Katastrophenfall aktualisiert.

| Hersteller | Produkt | Support-Nummer (regional) | Website des Herstellers |
|---|---|---|---|
| Cisco | Netzwerkswitches, Router, Server | +1 800 553 2447<br>+61 2 8446 7411<br>+32 2 704 5555 | http://www.cisco.com/ |
| Dell | Server | 1-800-624-9896<br>+1800 394 7488<br>020 674 45 00 | http://www.dell.com/ |
| NetApp | Speicherung | 888.463.8277<br>800.44.638277<br>800.800.80.800 | http://www.netapp.com/ |
| Juniper | Firewall | 1-888-314-5822<br>0800 022 3531<br>001-800-2586-4737 | http://www.juniper.net/ |
| A10 | Load Balancers (Lastverteiler) | 1-408-325-8676 | http://www.a10networks.com/ |
| Equinix | Rechenzentren | 1.866.378.4649<br>+31.(0).20.808.0015<br>800.852.3382 | http://www.equinix.com/ |
| Internap | IP & CDN | 1+877.843.4662<br>00-800-0044-0055<br>001-800-0044-0055 | http://www.internap.com/ |
| Palo Alto | Virenschutz | US: (866) 898-9087<br>Int'l: +1 (408) 738-7799<br>EMEA +31 20 808 4600<br>APAC: +65 3158 5600 | http://www.paloaltonetworks.com/ |