Notfallrichtlinie von Ex Libris

Alle in diesem Dokument enthaltenen Informationen sind vertrauliche Informationen von Ex Libris.

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 und vertraulichen Zwecken. Die hierin enthaltenen Informationen können Betriebsgeheimnisse enthalten 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. Diese Informationen erfolgen OHNE GEWÄHR. Sofern nicht anderweitig vereinbart, haftet Ex Libris nicht für Schäden aus bzw. im Zusammenhang mit der Verwendung dieses Dokumentes, einschließlich und ohne Einschränkung Folgeschäden, Bußgelder, indirekter oder direkter Schäden.

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

Marken

„Ex Libris", The Ex Libris Bridge to Knowledge, Primo, Aleph, Voyager, SFX, MetaLib, Verde, DigiTool, Rosetta, bX, URM, Alma, 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.

Copyright Ex Libris Ltd., 2014. Alle Rechte vorbehalten.

Webadresse: http://www.exlibrisgroup.com

Inhalt

1) Einführung 4
2) Zweck 4
3) Compliance 4
4) Prüfung und Aktualisierung der Richtlinie 4
5) Definitionen 4
6) Notfallmanagement-Team (SIRT) 5
7) Notfallmanagement 6
   7.1. Meldung und Erkennung 6
   7.2. Beurteilung des Schweregrads 8
   7.3. Bekanntgabe/Kommunikation 9
   7.4. Begrenzung 10
   7.5. Abhilfemaßnahmen 11
   7.6. Abschluss des Vorfalls 12
   7.7. Erfahrungsauswertung 12
   7.8. Abschlussbericht 13
8) Meldung von Verletzungen des Schutzes Personenbezogener Daten 13
   8.1. Executive Incident Management Team (EIMT) 13
   8.2. Maßnahmen im Falle einer Verletzung des Schutzes personenbezogener Daten 14
9) Anlage 1- Abschlussbericht 15

Alle in diesem Dokument enthaltenen Informationen sind vertrauliche Informationen von Ex Libris.

1) Einführung

Ex Libris arbeitet aktiv daran, die Sicherheit und Integrität aller in der Cloud-Umgebung von Ex Libris gespeicherten Daten zu wahren. Die Sicherheit kann durch zufällige oder absichtliche Handlungen gefährdet werden. Gefährdungen drohen sowohl von außerhalb als auch seitens der Belegschaft. Eine Gefährdung kann durch Präventivmaßnahmen verringert, jedoch nicht beseitigt werden. Ex Libris muss in der Lage sein, Sicherheitsvorfälle zu erkennen, zu beheben, zu melden und aus ihnen zu lernen. Diese Richtlinie legt einheitliche Abläufe zum Umgang mit Sicherheitsvorfällen fest.

2) Zweck

Mit dieser Richtlinie soll sichergestellt werden, dass Ex Libris angemessen auf tatsächliche bzw. vermutete Sicherheitsvorfälle im Zusammenhang mit den Cloudsystemen und Daten von Ex Libris reagiert. Diese Richtlinie legt die Abläufe fest, denen die Mitarbeiter von Ex Libris folgen müssen, um zu gewährleisten, dass Sicherheitsvorfälle erkannt, begrenzt, untersucht und behoben werden. Sie legt darüber hinaus Abläufe zur Dokumentierung sowie zu einer angemessenen internen und externen Bekanntgabe und Kommunikation fest, so dass ein Lernprozess im Unternehmen stattfinden kann. Schließlich werden Zuständigkeiten und Verantwortlichkeiten für alle Stufen des Notfallmanagements festgelegt.

3) Compliance

Verstöße gegen diese Richtlinie werden dem Senior Management von Ex Libris gemeldet und können Disziplinarmaßnahmen zur Folge haben.

4) Prüfung und Aktualisierung der Richtlinie

Diese Richtlinie und die ihr unterliegenden Abläufe werden mindestens einmal jährlich überprüft und gegebenenfalls aktualisiert.

5) Definitionen

Sicherheitsvorfall - Ein Sicherheitsvorfall ist jedes tatsächliche bzw. vermutete Ereignis, das die Sicherheit der Cloud-Informationen bzw. der diese Informationen verarbeitenden, speichernden oder übermittelnden Systeme von Ex Libris nachteilig beeinträchtigt.

Sicherheitsvorfälle beinhalten, sind jedoch nicht beschränkt auf folgende Ereignisse:

- Versuche (sowohl fehlgeschlagene als auch erfolgreiche Versuche), sich unbefugten Zugang zu einem System bzw. dessen Daten zu verschaffen
- Ein mit Schadsoftware, wie z.B. einem Wurm, Virus oder Trojaner infiziertes System
- Diebstahl, Verlust bzw. unbefugte Übermittlung von Daten an Personen, die zum Erhalt dieser Daten nicht berechtigt sind
- Ungewollte Unterbrechung bzw. DoS (Denial of Service)-Angriff
- Änderungen der Daten bzw. Systemhardware, Firmware oder Software ohne das Wissen, die Anweisung oder Zustimmung von Ex Libris

Alle in diesem Dokument enthaltenen Informationen sind vertrauliche Informationen von Ex Libris.

6) Notfallmanagement-Team (Security Incident Response Team - SIRT)

Das Notfallmanagement-Team (SIRT) besteht aus Mitarbeitern von Ex Libris mit Entscheidungsbefugnis, die vom Ex Libris-COO beauftragt werden und befugt sind, die in diesem Dokument beschriebenen Abläufe zu unterstützen.

Das SIRT besteht aus Vertretern folgender Bereiche:

- Chief Information Security Officer (CISO) - Leitung des Teams
- Cloud Operation Group (COG)
- Cloud Engineering Group (CEG)
- 24 x 7 HUB
- BU Development (URM bzw. URD)
- Global Support Organisation (GSO)
- Externer Sicherheitsberater (bei Bedarf)

Unter der Leitung des CISO von Ex Libris verfolgt das SIRT folgende Ziele:

- Koordination und Beaufsichtigung der Notfallmaßnahmen entsprechend den Anforderungen der Sicherheitsrichtlinie von Ex Libris und den gesetzlichen Vorschriften
- Verringerung der potenziell negativen Auswirkungen solcher Vorfälle auf Ex Libris und deren Kunden
- Behebung bzw. Koordinierung der Behebung von durch den Vorfall verursachten Schäden
- Wiederherstellung der Leistungen in einen normalisierten und sicheren Betriebsstatus
- Gegebenenfalls Sicherung von Beweisen des Vorfalls
- Klare und zeitnahe Benachrichtigung aller betroffenen Parteien
- Aktive Maßnahmen zur Vermeidung zukünftiger Vorfälle

Alle in diesem Dokument enthaltenen Informationen sind vertrauliche Informationen von Ex Libris.

7) Notfallmanagement

Das Notfallmanagement folgt mehreren Stufen: Meldung/Erkennung, Beurteilung des Schweregrades, Bekanntgabe /Kommunikation, Begrenzung, Abhilfemaßnahmen, Abschluss des Vorfalls und Erfahrungsauswertung.

Einige der oben beschriebenen Stufen können gleichzeitig oder in anderer Reihenfolge erfolgen, abhängig von den Umständen des Sicherheitsvorfalls. Darüber hinaus können die während des Vorfalls protokollierten Informationen regelmäßige Aktualisierungen erfordern und spezifische Angaben wie z.B. der Schweregrad, können sich im Laufe zukünftiger Analysen ändern.

7.1. Meldung und Erkennung

Ein Vorfall tritt ein, wenn dem Chief Information Security Officer von Ex Libris ein solcher Sicherheitsvorfall gemeldet wird (sofern der CISO nicht verfügbar ist, werden Meldungen an den Director of Cloud Operation von Ex Libris weitergeleitet). Diese Meldung kann von einem Mitarbeiter von Ex Libris, einer automatischen Systemdiagnose, einem von einem Kunden eingereichten Support Ticket oder über andere Kanäle erfolgen.

Kunden, die einen Sicherheitsvorfall erkannt haben, sollten Ex Libris über das Salesforce CRM-System benachrichtigen. Im Falle eines Systemausfalls wird der Vorfall automatisch dem 24x7 Hub unter Angabe der Art des Vorfalls und weiterer Einzelheiten gemeldet.

Über die Meldungen vermuteter bzw. bestätigter Sicherheitsvorfälle seitens der Mitarbeiter bzw. Kunden von Ex Libris hinaus werden gegebenenfalls ungewöhnliche Ereignisse beobachtet, die potenzielle Sicherheitsverstöße anzeigen. Ex Libris unternimmt zahlreiche Anstrengungen zur Erkennung von ungewöhnlichen Ereignissen, um deren Auswirkungen zu minimieren. Hierzu zählen unter anderem:

- Überwachung von Sicherheits-Mailinglisten und Webseiten für Gefahrenwarnungen (zum Beispiel das SANS Internet Storm Center - isc.sans.org)
- Überwachung externer Informationsquellen zu neuen Verwundbarkeiten und Systemeinbrüchen sowie von Vorfällen in anderen Unternehmen
- Anwendung passiver Erkennungstechniken, wie z.B. Netzwerkflussanalysen (Auslastungsgrenzen, Kommunikation mit bekannten bösartigen Seiten etc.); Protokolldateianalyse (Betriebssystem, Systemdienste, Datenbanken, Anwendungen, Netzwerkgeräte etc.); Einbruchserkennungs-/Einbruchsverhinderungssysteme und Überwachung der Warnmeldungen von Sicherheitssystemen (Firewalls, Virenschutzprogramme, Einbruchserkennungs-/Einbruchsverhinderungssysteme etc.)
- Anwendung aktiver Erkennungstechniken wie Port-Scans, die nach unüblichen Diensten suchen, Verwundbarkeits-Scans, Überwachung der Netzwerk-Performance (zum Beispiel Erkennung eines überlasteten Netzwerksegmentes) und Verifizierung der Datei-Integrität zur Erkennung von Änderungen an wichtigen Dateien

Nach der Meldung eines vermuteten bzw. bestätigten Sicherheitsvorfalls holt der CISO so viele der nachstehenden Informationen wie möglich ein.

Alle in diesem Dokument enthaltenen Informationen sind vertrauliche Informationen von Ex Libris.

Zu dokumentierend	Beschreibung/Anmerkungen
Referenz	Verwenden Sie die zugewiesene Salesforce-Case-Nummer
Art des Vorfalls	Zum Beispiel: ▪ Betroffenes System ▪ Betroffene Nutzer-Zugangsdaten ▪ Netzwerkangriffe (DOS, Scanning, Sniffing) ▪ Schadsoftware (Viren, Würmer, Trojaner) ▪ Verlust/Diebstahl von Geräten ▪ Physischer Einbruch ▪ Social Engineering (Phishing) ▪ Richtlinienverstoß ▪ Datenleck
Zeitangaben	Datum/Uhrzeit der Entdeckung des Vorfalls, Datum/Uhrzeit der Meldung des Vorfalls, Datum/Uhrzeit des Auftretens des Vorfalls
Wer bzw. was hat den Vorfall gemeldet	Kontaktdaten des Meldenden: vollständiger Name, Unternehmen, E-Mail-Adresse, Telefonnummer und Standort. Sofern die Meldung über ein automatisches System erfolgt, geben Sie den Namen der Software/des Produktes, den Namen des Hosts, auf dem die Software installiert ist, den physischen Standort des Hosts, die Host-/CPU-ID sowie die Netzwerkadresse des Hosts ein.
Kontaktdaten	Geben Sie die Kontaktdaten aller in den Vorfall involvierten Parteien an.

Alle in diesem Dokument enthaltenen Informationen sind vertrauliche Informationen von Ex Libris.

Zu dokumentierende Informationen	Beschreibung/Anmerkungen
Detaillierte Beschreibung des Vorfalls	Geben Sie so viele Informationen wie möglich an, z.B.: ▪ Beschreibung des Vorfalls (wie wurde er erkannt, was ist passiert) ▪ Beschreibung der betroffenen Ressourcen ▪ Beschreibung der betroffenen Unternehmen ▪ Geschätzte technische Auswirkungen des Vorfalls (d.h. gelöschte Daten, Systemzusammenbruch, nicht verfügbare Anwendung) ▪ Zusammenfassung durchgeführter Abhilfemaßnahmen ▪ Sonstige kontaktierte Unternehmen ▪ Ursache des Vorfalls, sofern bekannt (falsch konfigurierte Anwendung, ungepatchter Host etc.) ▪ Liste gesammelter Beweise ▪ Official Common Vulnerabilities and Exposures (CVE®) (Standardisierte Verwundbarkeiten und Sicherheitslücken) ▪ Beschreibung, wie die Sicherheitslücke geschlossen werden kann
Identifizierung des/der Host(s)	Quelle des Vorfalls: Liste der als Quelle identifizierten Hostnamen/IP-Adressen Ziel des Angriffs: Hostname/IP-Adresse (Anmerkung: Das Angriffsziel darf für Vorfälle, die personenbezogene Daten betreffen, nicht aufgeführt werden)

Sobald der CISO den Eintritt eines Vorfalls bestätigt hat, aktiviert er dieses Verfahren unverzüglich und beruft das SIRT-Team ein.

7.2. Beurteilung des Schweregrads

Der Schweregrad eines Vorfalls ist eine subjektive Messung seiner Auswirkungen auf den Betrieb bzw. die Integrität der Cloud-Dienste von Ex Libris und deren Kundendaten. Er bestimmt die Priorität für die Behebung des Vorfalls sowie Zeitaufwand und Umfang der Maßnahmen.

Bei der Ermittlung des Schweregrads eines Vorfalls werden die folgenden Faktoren berücksichtigt:

A. **Ausmaß der Leistungsunterbrechung** - Wie viele Systeme bzw. Institutionen sind betroffen?
B. **Ausbreitungswahrscheinlichkeit** - Wie wahrscheinlich ist es, dass sich die Schadsoftware bzw. die negativen Auswirkungen ausbreiten oder auf andere Systeme übergreifen?
C. **Freisetzung bzw. Gefährdung personenbezogener Daten** - Waren personenbezogene Daten betroffen?
D. **Abhilfemaßnahmen** - Welche Maßnahmen und welche Dringlichkeit sind erforderlich?

Alle in diesem Dokument enthaltenen Informationen sind vertrauliche Informationen von Ex Libris.

Für den Umgang mit Vorfällen gelten drei Schweregrade: hoch, mittel und gering

Schweregrad	Symptome
Hoch	A. Netzwerk- bzw. Systemausfall mit erheblichen Auswirkungen auf die Nutzer bzw. den Betrieb der Cloud-Dienste von Ex Libris. B. Hohe Ausbreitungswahrscheinlichkeit. C. Wahrscheinliche oder tatsächliche Freisetzung bzw. Gefährdung personenbezogener Daten D. Erfordert unverzügliche Abhilfemaßnahmen zur Vermeidung weiterer Gefährdungen von Daten und nachteiliger Auswirkungen auf Netzwerk und übrige Systeme.
Mittel	A. Gewisse nachteilige Auswirkungen auf den Betrieb der Cloud-Dienste von Ex Libris. B. Die nachteiligen Auswirkungen wurden lokalisiert bzw. begrenzt oder geringes Ausbreitungsrisiko. C. Keine offensichtliche Freisetzung oder Gefährdung personenbezogener Daten. D. Es sind Abhilfemaßnahmen erforderlich, diese müssen jedoch nicht sofort erfolgen.
Gering	A. Geringe Auswirkungen auf einen kleinen Nutzerkreis bzw. den Betrieb der Cloud-Dienste von Ex Libris. B. Vollständig lokalisiert, nur wenige Personen betroffen, kein bzw. nur geringes Risiko für andere Systeme. C. Kein Verlust bzw. keine Gefährdung personenbezogener Daten. D. Es sind Abhilfemaßnahmen erforderlich.

Anmerkung: Eine Schweregradklassifizierung von Vorfällen kann sich aufgrund nachfolgender Ereignisse oder erweiterter Kenntnis über den Vorfall ändern.

7.3. Bekanntgabe/Kommunikation

Die Leitung des SIRT ergreift Maßnahmen, um die betroffenen internen und externen Parteien entsprechend der jeweiligen Notwendigkeit zu informieren.

Interne Bekanntgabe (innerhalb von Ex Libris)

- Der SIRT-Leiter veranlasst jegliche interne Kommunikation.
- Die SIRT-Leitung informiert das Senior Management, die Cloud-Direktoren, die Support-Direktoren sowie den 24x7 HUB über den Vorfall und übermittelt laufende Statusberichte.

Alle in diesem Dokument enthaltenen Informationen sind vertrauliche Informationen von Ex Libris.

Externe Bekanntgabe

- Bei einem Notfall der Kategorie „hoch" wird/werden der/die betroffene/n Kunde/n schnellstmöglich, jedoch spätestens vierundzwanzig (24) Stunden nachdem Ex Libris Kenntnis von dem schweren Sicherheitsvorfall erlangt hat, benachrichtigt.
- Die Meldung beinhaltet soweit möglich:
  - Zeitpunkt des Vorfalls (Datum/Uhrzeit der Entdeckung des Vorfalls)
  - Art des Sicherheitsvorfalls (Netzwerkangriff, Wurm/Trojaner etc.)
  - Beschreibung des Vorfalls (wie wurde er erkannt, was ist passiert)
- Im Falle einer Verletzung personenbezogener Daten erfolgt die externe Meldung gemäß der „Richtlinie für Meldungen einer Verletzung des Schutzes personenbezogener Daten" (siehe Abschnitt 8)
- Nach der ersten Meldung hält Ex Libris den/die betroffenen Kunden regelmäßig über den Stand der Untersuchung des Vorfalls auf dem Laufenden.
- Die betroffenen Kunden erhalten einen Notfallbericht, einschließlich der Ergebnisse der Ursachenanalyse, der von Ex Libris vorgenommen Abhilfemaßnahmen sowie aller seitens des/der Kunden zu ergreifenden Maßnahmen zur Minimierung potenzieller Schäden. Solche Berichte erfolgen zeitnah, spätestens jedoch fünfzehn (15) Tage nach der Entdeckung des Vorfalls durch Ex Libris.
- Alle Informationen, die Ex Libris den betroffenen Kunden im Hinblick auf den Sicherheitsvorfall übermittelt, sind vertrauliche Informationen von Ex Libris und müssen als solche gekennzeichnet und behandelt werden.

7.4. Begrenzung

Das SIRT ermittelt und ergreift geeignete Maßnahmen, die zu einer raschen Begrenzung der unmittelbaren Auswirkungen auf die Cloud-Dienste und Kunden von Ex Libris erforderlich sind.

Begrenzungsmaßnahmen haben primär folgende Ziele:
- Abwehr der unmittelbaren Gefahr
- Verhinderung einer Ausbreitung des Vorfalls
- Verhinderung weiterer Schäden an dem betroffenen System und/oder den Daten
- Beschränkung der Kenntnis von dem Vorfall auf befugte Mitarbeiter
- Sicherung von Informationen im Zusammenhang mit dem Vorfall

Zu den Begrenzungsmaßnahmen im Falle eines unbefugten Zugriffs zählen unter anderem folgende:

Alle in diesem Dokument enthaltenen Informationen sind vertrauliche Informationen von Ex Libris.

A. Begrenzungsmaßnahmen - Unbefugter Zugriff Gegebenenfalls erforderliche Maßnahmen zur Begrenzung der Gefahr für die Systeme, die von einem unbefugten Zugriff betroffen sein könnten
A1. Trennung der Verbindung des Systems bzw. der Hosts vom Netzwerk bzw. Sperren des
A2. Isolierung der betroffenen IP-Adresse vom Netzwerk
A3. Sofern möglich, Erfassen und Sichern von System-, Host- und Anwendungsprotokollen sowie Netzwerkflüssen zwecks Überprüfung
A4. Deaktivierung der betroffenen Anwendung(en)
A5. Unterbrechung bzw. Abschalten des Remote-Zugangs
A6. Einstellen der Dienste bzw. Schließen der Ports, die zu dem Vorfall beitragen
A7. Abschalten des/der Hosts, sofern keine anderweitige Isolierung möglich ist
A8. Meldung des Status und aller ergriffenen Maßnahmen an das SIRT

7.5. Abhilfemaßnahmen

Nach einer Begrenzung der Situation geht das SIRT dazu über, durch den Sicherheitsvorfall verursachte Schäden zu beheben und die Ursache zu ermitteln.

Die Abhilfemaßnahmen dienen primär folgenden Zielen:

- Sicherung der Cloud-Umgebung von Ex Libris
- Wiederherstellung des normalen Zustandes der Cloud-Umgebung von Ex Libris

Zu den Abhilfemaßnahmen im Falle eines unbefugten Zugriffs zählen unter anderem folgende:

A. Abhilfemaßnahmen - Unbefugter Zugriff Alle Tätigkeiten, die notwendig sind, um nach einem unbefugten Zugriff einen normalen und sicheren Betriebsstatus wiederherzustellen
A1. Änderung der Passwörter/Passphrasen aller lokalen Benutzer- und Administratoraccounts bzw. gegebenenfalls anderweitige Deaktivierung der Accounts
A2. Änderung der Passwörter/Passphrasen aller Administratoraccounts, die dasselbe Passwort/dieselbe Passphrase für mehrere Anwendungen bzw. Systeme nutzen (Server, Firewalls, Router)
A3. Zurückführung des Systems in einen sicheren Status
A4. Wiederherstellung von Systemen mit Daten hoher Integrität
A5. Gegebenenfalls Abänderung der Zugangskontrolllisten
A6. Gegebenenfalls Implementierung von IP-Range-Filtern
A7. Gegebenenfalls Abänderung/Implementierung von Firewall-Regelsätzen
A8. „Schärfung" des Sicherheitsbewusstseins aller Mitarbeiter
A9. Überwachung/Scan von Systemen, um sicherzustellen, dass die Probleme behoben wurden
A10. Meldung des Status und aller ergriffenen Maßnahmen an das SIRT

Alle in diesem Dokument enthaltenen Informationen sind vertrauliche Informationen von Ex Libris.

7.6. Abschluss des Vorfalls

Alle Tätigkeiten im Zusammenhang mit dem Vorfall - vom Eingang der ersten Meldung bis zur Erfahrungsauswertung - sind zu dokumentieren. Der SIRT-Leiter trägt dafür Sorge, dass alle Ereignisse protokolliert werden, die entsprechenden Protokolle zur Vorbereitung und Durchführung der Erfahrungsauswertung zusammengetragen und zwecks Prüfung verwahrt werden. Die Mitglieder des SIRT können hiermit beauftragt werden.

Allgemeine Zusammenfassung des Vorfalls
Zusammenfassung des Vorfalls unter allgemeiner Beschreibung von Ereignissen, Angabe ungefährer Zeiten, involvierter Parteien, Behebung des Vorfalls, erforderlicher externer Bekanntgaben und Empfehlungen zur Vermeidung und Abhilfe.

Detaillierte Prüfung des Vorfalls
Beschreibung von Ereignissen des Vorfalls unter Angabe spezifischer Zeiten, involvierter Mitarbeiter, Zeitaufwand für unterschiedliche Tätigkeiten, Auswirkungen auf Kunden und Nutzer (z.B. keine Verfügbarkeit des Systems, Probleme in der betrieblichen Kontinuität), Folgebesprechungen, getroffener Entscheidungen und Beauftragungen, aufgetretener Probleme, erfolgreicher und erfolgloser Maßnahmen, erforderlicher bzw. empfohlener Information des Kunden (einschließlich Updates im „Systemstatus"-Portal), eingeleiteter Maßnahmen zur Begrenzung und Abhilfe, Empfehlungen zur Vermeidung und Abhilfe (kurz- und langfristig), Identifizierung von Lücken in Richtlinien und Abläufen, Ergebnisse der Erfahrungsauswertung.

Aufbewahrung
Alle relevanten Unterlagen werden vom Leiter des SIRT in einem zentralen Archiv für einen Zeitraum entsprechend der jeweils für Ex Libris geltenden Praxis aufbewahrt. Der Zugang zu den Unterlagen und dem Archiv ist üblicherweise beschränkt auf die Mitglieder des SIRT und die Cloud-Manager von Ex Libris.

7.7. Erfahrungsauswertung

Die Leitung des SIRT wird nach der Behebung jedes mittleren und schweren Vorfalls einen sogenannten Lessons Learned Review (Besprechung zur Auswertung der Erfahrungen) abhalten. Diese Besprechung sollte 2-3 Wochen nach Behebung des Vorfalls stattfinden. Bei dieser Erfahrungsauswertung handelt es sich um eine Untersuchung des Vorfalls und aller damit verbundenen Tätigkeiten und Ereignisse. Alle im Zusammenhang mit dem Vorfall ausgeführten Tätigkeiten sind mit Blick auf eine Verbesserung des Notfallmanagementprozesses insgesamt zu prüfen.
Die Empfehlungen des SIRT zu Änderungen von Richtlinien, Prozessen, Sicherheitsvorkehrungen etc. dienen sowohl als Input, als auch als Nebenprodukt dieser Prüfung. Der Fokus liegt hierbei auf der Beseitigung des Problems und nicht auf der Suche nach einem Schuldigen („Fix the problem, not the blame"). Alle Besprechungen, Empfehlungen und Beauftragungen sind für eine Weitergabe an die Cloud Operation und Engineering Groups von Ex Libris sowie für eine Nachbereitung durch die SIRT-Leitung zu dokumentieren. Alle Protokolle und Unterlagen werden jährlich von einem ISO-Prüfer im Rahmen des ISO-27001-Zertifizierungsverfahrens geprüft.

Alle in diesem Dokument enthaltenen Informationen sind vertrauliche Informationen von Ex Libris.

7.8. Abschlussbericht

- Sicherheitsvorfälle der Kategorie „hoch" erfordern die Erstellung eines Abschlussberichtes (darüber hinaus kann der COO eine solchen für jeden Sicherheitsvorfall anfordern).
- Dem CISO obliegt die Erstellung des Abschlussberichtes.
- Der Bericht sollte eine umfassende Beschreibung des Vorfalls und dessen Ausmaßes, die Auswirkungen auf die Cloud-Dienste und Kunden von Ex Libris, sowie die angewandten Maßnahmen zur Vermeidung eines zukünftigen Auftretens und Empfehlungen für weitere Maßnahmen enthalten.
- Der COO prüft alle Empfehlungen des Berichtes und ermittelt zusätzliche Follow-Up-Maßnahmen.
- Abschlussberichte sind unter Verwendung des in Anlage 1 spezifizierten Formulars an den COO zu richten und als vertraulich zu kennzeichnen.

8) Meldung von Verletzungen des Schutzes Personenbezogener Daten

Für Vorfälle, die bei denen eine Verletzung vertraulicher personenbezogener Daten vermutet wird bzw. bekannt ist, gelten über die üblichen, in diesem Dokument behandelten Notfallmaßnahmen hinaus besondere Abläufe.

8.1. Executive Incident Management Team (EIMT)

Das **Executive Incident Management Team (EIMT - Leitendes Notfallmanagement-Team)** beaufsichtigt den Umgang mit den von einem Sicherheitsvorfall betroffenen personenbezogenen Daten (d.h. die **Persönlich Identifzierbaren Daten - PID).** Das EIMT kann auch die Behebung anderer schwerwiegender Vorfälle überwachen, wird aber vorranging zur Behebung von Vorfällen eingesetzt, die personenbezogene Daten betreffen. Zweck des EIMT ist es, die Notfallmaßnahmen in leitender Funktion zu begleiten: a) um eine angemessene, zeitnahe und rechtmäßige Behebung sicherzustellen, b) um Entscheidungen im Zusammenhang mit dem Vorfall zu treffen und c) um die entsprechenden Parteien zu benachrichtigen. Das Team besteht aus:

1) Dem Chief Operating Officer von Ex Libris (COO)
2) Dem Leiter des betroffenen Geschäftsbereichs (URD bzw. URM)
3) Dem Leiter der Rechtsabteilung von Ex Libris
4) Vertretern der Produktmanagement-Teams

Alle in diesem Dokument enthaltenen Informationen sind vertrauliche Informationen von Ex Libris.

8.2. Maßnahmen im Falle einer Verletzung des Schutzes personenbezogener Daten

1) Sofern das SIRT feststellt, dass eine Verletzung des Schutzes personenbezogener Daten erfolgt ist bzw. vermutet wird, informiert das SIRT unverzüglich den COO.

2) Das SIRT veranlasst zusätzliche Analysen, um so viele Informationen wie möglich über den Vorfall zu sammeln und trägt dafür Sorge, dass Beweise ordnungsgemäß gesichert werden.

3) Sofern nach der Analyse der COO und das SIRT bestätigt haben, dass keine Verletzung des Schutzes personenbezogener Daten erfolgt ist, sind keine weiteren Maßnahmen erforderlich und die üblichen Notfallmaßnahmen können fortgesetzt werden. Die Sicherheit des betroffenen Systems sollte dennoch sorgfältig überprüft werden.

4) Sofern durch die Analyse eine Verletzung des Schutzes personenbezogener Daten bestätigt wird, beruft der COO schnellstmöglich das EMIT ein.

5) Das EMIT veranlasst entsprechende Maßnahmen unter Berücksichtigung folgender Aspekte:
   - Feststellung, welche Kunden informiert werden müssen und wie schnell und auf welche Weise dies geschehen soll
   - Feststellung des genauen Ausmaßes der Verletzung des Schutzes personenbezogener Daten (welche Personen und Daten waren betroffen etc.)
   - Benachrichtigung des/der betroffenen Kunden unter Angabe des Verstoßes, der Art der betroffenen Daten und sonstiger Informationen, die der Kunde gegebenenfalls im Hinblick auf die betroffenen Personen verlangt.
   - Unterstützung des/der betroffenen Kunden bei erforderlichen Meldungen an Dritte (wie z.B. Inhalt öffentlicher Stellungnahmen, Benachrichtigung betroffener Personen, Behörden oder sonstiger Stellen entsprechend den gesetzlichen bzw. behördlichen Vorschriften)

Alle in diesem Dokument enthaltenen Informationen sind vertrauliche Informationen von Ex Libris.

Anlage 1 - Abschlussbericht

Salesforce ID-Nummer des Vorfalls: YYYYYYY

Schweregrad des Vorfalls:

Überschrift des Vorfalls:

Notfallmanager (Name, Titel, E-Mail, Telefon):

Datum der erstmaligen verdächtigen/böswilligen Aktivität:

Datum der Meldung des Vorfalls:

Datum der vollständigen Begrenzung des Vorfalls:

Abschlussprüfung:

Datum:
Teilnehmer:

Datum des Abschlusses der Notfallmaßnahmen:

Abschlussbericht übermittelt von (Name, Titel, E-Mail, Telefon):

Abschlussbericht verteilt an:

Datum der Übermittlung des Abschlussberichtes

Zusammenfassung des Vorfalls:
Allgemeine Zusammenfassung der Geschehnisse unter Angabe der Art und Weise des Auftretens des Sicherheitsvorfalls und dessen Ausmaßes (z.B. betroffene Personen und Systeme, Daten wesentlicher Meilensteine etc.). Detaillierte Angaben, wie z.B. ein Zeitplan, können dem Bericht am Ende als Anhang beigefügt werden.

Erkennung des Vorfalls:
Beschreiben Sie kurz, wie der Vorfall zuerst entdeckt wurde (wann, wie und von wem).

Begrenzung des Vorfalls & Abhilfemaßnahmen:
Beschreiben Sie, wie der Vorfall begrenzt (Verhinderung der Ausbreitung und/oder weiteren Verursachung von Schäden) und behoben (aus den infizierten Hosts beseitigt) wurde. Erläutern Sie auch Wiederherstellungsmaßnahmen.

Alle in diesem Dokument enthaltenen Informationen sind vertrauliche Informationen von Ex Libris.

Meldung des Vorfalls
Sofern bei dem Vorfall in meldepflichtiger Weise der Schutz personenbezogener Daten verletzt wurde bzw. vermutet wird, beschreiben Sie, wie und wann die betroffenen Kunden benachrichtigt wurden.

Auswertung des Vorfalls
Führen Sie Maßnahmen zur Vermeidung zukünftiger Vorfälle, Erfahrungen und sonstige Empfehlungen aus dem Vorfall sowie der Abschlussprüfung auf.

A. Maßnahmen zur Vermeidung zukünftiger Vorfälle

i.

B. Erfahrungsauswertung

i.

C. Sonstige Empfehlungen

i.

Anlagen
Fügen Sie sonstige relevante Informationen über den Vorfall hinzu, die archiviert werden sollen.

Alle in diesem Dokument enthaltenen Informationen sind vertrauliche Informationen von Ex Libris.