Ex Libris' Security Incident Response Policy

CONFIDENTIAL INFORMATION

The information herein is the property of Ex Libris Ltd. or its affiliates and any misuse or abuse will result in economic loss. DO NOT COPY UNLESS YOU HAVE BEEN GIVEN SPECIFIC WRITTEN AUTHORIZATION FROM EX LIBRIS LTD.

This document is provided for limited and restricted purposes. The information herein may include trade secrets and is confidential

DISCLAIMER

The information in this document will be subject to periodic change and updating. Please confirm that you have the most current documentation. There are no warranties of any kind, express or implied, provided in this documentation. This information is provided AS IS. Ex Libris shall not be liable for any damages by reason of or in connection with this document, including, without limitation, consequential, punitive, indirect or direct damages.

Any references in this document to third-party material (including third-party Web sites) are provided for convenience only and do not in any manner serve as an endorsement of that third-party material or those Web sites. Ex Libris has no liability for such materials or sites.

TRADEMARKS

"Ex Libris," the Ex Libris Bridge to Knowledge , Primo, Aleph, Voyager, SFX, MetaLib, Verde, DigiTool, Rosetta, bX, URM, Alma , and other marks are trademarks or registered trademarks of Ex Libris Ltd. or its affiliates.

The absence of a name or logo in this list does not constitute a waiver of any and all intellectual property rights that Ex Libris Ltd. or its affiliates have established in any of its products, features, or service names or logos.

Trademarks of various third-party products, which may include the following, are referenced in this documentation. Ex Libris does not claim any rights in these trademarks. Use of these marks does not imply endorsement by Ex Libris of these third-party products, or endorsement by these third parties of Ex Libris products.

Oracle is a registered trademark of Oracle Corporation.

UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Ltd.

Microsoft, the Microsoft logo, MS, MS-DOS, Microsoft PowerPoint, Visual Basic, Visual C++, Win32, Microsoft Windows, the Windows logo, Microsoft Notepad, Microsoft Windows Explorer, Microsoft Internet Explorer, and Windows NT are registered trademarks and ActiveX is a trademark of the Microsoft Corporation in the United States and/or other countries.

Unicode and the Unicode logo are registered trademarks of Unicode, Inc.

Google is a registered trademark of Google, Inc.

Web address: http://www.exlibrisgroup.com

Table of Contents

Record of Changes

Type of Information	Document Data
Document Title:	Ex Libris' Security Incident Response Policy
Document Owner:	Eyal Alkalay – Ex Libris Cloud Engineering Director
Approved by:	Yair Amsterdam – Ex Libris Chief Operating Officer
Issued:	18-Apr-2011
Reviewed & Revised:	8-March-2016

Document Distribution and Review

The document owner will distribute this document to all approvers when it is first created and as changes or updates are made. This document will be reviewed and updated annually or upon written request by an approver or stakeholder. Questions or feedback about this document can be directed to the owner or a listed approver.

1) Introduction

Ex Libris, a ProQuest company, proactively strives to maintain the security and integrity of all data it holds in the Ex Libris cloud environment. Security threats can arise from accidental or intentional acts. Threats may come from external parties or from the workforce. While preventive measures lessen a threat, they cannot eliminate it. Ex Libris must be able to detect, respond to, report, and learn from security incidents. This policy defines a consistent way to handle security incidents.

2) Purpose

The aim of this policy is to ensure that Ex Libris reacts appropriately to any actual or suspected security incidents relating to Ex Libris cloud systems and data. This policy defines the steps that Ex Libris personnel must use to ensure that security incidents are identified, contained, investigated, and remedied. It also provides a process for documentation, appropriate reporting internally and externally, and communication so that organizational learning occurs. Finally, it establishes responsibility and accountability for all steps in the process of addressing security incidents.

3) Compliance

Violations of this policy will be reported to Ex Libris senior management and may result in disciplinary action.

4) Policy Review and Update

This policy and its supporting procedures, will be reviewed at least annually, and updated as required.

5) Definitions

Security Incident - A security incident is any real or suspected event that may adversely affect the security of Ex Libris cloud information or the systems that process, store, or transmit that information.

A Security Incident includes, but is not restricted to, the following:

- Attempts (either failed or successful) to gain unauthorized access to a system or its data
- A system infected with malware, such as a worm, virus, or Trojan horse
- Theft, loss, or unauthorized transfer of data to those who are not entitled to receive that data
- Unwanted disruption or denial-of-service (DoS) attack
- Changes to data or system hardware, firmware, or software without Ex Libris' knowledge, instruction, or consent

6) Security Incident Response Team (SIRT)

The Security Incident Response Team (SIRT) is comprised of Ex Libris' individuals with decision-making authority who are appointed by Ex Libris' COO with the responsibility of assisting in the process described within this document.

The SIRT will consist of representatives from the following areas:

- Chief Information Security Officer (CISO) - Team Lead
- Cloud Operation Group (COG)
- Cloud Engineering Group (CEG)
- 24 x 7 HUB
- BU Development (URM or URD)
- Global Support Organization (GSO)
- External Security consultant (upon need)

Led by the Ex Libris' CISO, the SIRT's objectives are to:

- Coordinate and oversee the response to incidents in accordance with the requirements of Ex Libris' security policy and regulatory laws
- Minimize the potential negative impact on Ex Libris and Ex Libris' customers resulting from such incidents
- Repair, or coordinate the repair of, damage caused by the incident
- Restore services to a normalized and a secure state of operation
- Preserve evidence of the incident, as appropriate
- Provide clear and timely communication to all interested parties
- Take proactive steps to prevent future incidents.

7) Security Incident Response Procedure

Security incident response will follow several stages: reporting/detection, severity assessment, notification/communication, containment, corrective measures, incident closure, and lessons learned review.

Some of the stages described above may be taken concurrently or in a different order, depending on the circumstances of the security incident. Furthermore, the incident information logged throughout the incident may require periodic updates and specific information, such as severity level, may change as further analysis is performed.

7.1. Reporting and Detection

An incident begins when a security incident is reported to Ex Libris' Chief Information Security Officer (if the CISO is not available, reports are directed to Ex Libris' Director of Cloud Operation). This report could come from an Ex Libris employee, an automated system diagnostic, a support ticket submitted by a customer, or other means.

A customer who identified a security incident should notify Ex Libris via the Salesforce CRM system. In the case of a system disruption, the incident will be escalated to the 24x7 Hub automatically, with information on the nature of the incident and other details.

In addition to reports from Ex Libris employees or the customer community of suspected or confirmed security incidents, anomalous events may be detected that indicate potential security incidents. Ex Libris spends a great deal of effort to detect anomalous events early to minimize their impact. These efforts include:

- Monitoring security mailing lists and web sites for threat alerts (for example, the SANS Internet Storm Center — isc.sans.org)
- Monitoring external sources of information about new vulnerabilities and exploits, as well as incidents occurring at other organizations
- Employing passive detection techniques, such as network flow analysis (traffic volume thresholds, communication with known malicious sites, etc.); log file analysis (operating system, system services, databases, applications, network devices, etc.); intrusion detection/prevention systems, and monitoring alerts from security systems (firewalls, anti-virus protection, intrusion detection/prevention systems, etc.)
- Employing active detection techniques, such as port scans looking for unusual services, vulnerability scans, network performance monitoring (for example, noticing a congested network segment), and file integrity verification that detects changes to important files

When receiving a report of a suspected or confirmed security incident, the CISO will gather as much of the following information as possible:

Information to Be Documented	Description/Note
Reference	Use the assigned Salesforce case number
Type of incident	For example: ▪ Compromised System ▪ Compromised User Credentials ▪ Network Attacks (DOS, Scanning, Sniffing) ▪ Malware (Viruses, Worms, Trojans) ▪ Lost Equipment/Theft ▪ Physical Break-in ▪ Social Engineering (Phishing) ▪ Policy Violation ▪ Data Leakage
Incident timeline	Date/time that the incident was discovered Date/time that the incident was reported Date/time that the incident occurred (if known)
Who or what reported the incident	Contact information for the incident reporter: full name, affiliation, organizational, email address, phone number, and location. If an automated system reported the event, include the name of software/product, name of the host where the software is installed, physical location of the host, host/CPU ID of the host, network address of the host.
Incident contact information	List contact information for all parties involved in the incident.

Information to Be Documented	Description/Note
Detailed description of the incident	Include as much information as possible, such as: ▪ Description of the incident (how it was detected, what occurred) ▪ Description of the affected resources ▪ Description of the affected organizations ▪ Estimated technical impact of the incident (i.e., data deleted, system crashed, application unavailable) ▪ Summary of response actions performed ▪ Other organizations contacted ▪ Cause of the incident, if known (misconfigured app, unpatched host, etc.) ▪ List of evidence gathered ▪ Official Common Vulnerabilities and Exposures (CVE®) ▪ Description of how to reproduce the exploit
Identification of the host(s)	Source of the incident: List of sources' host names/IP addresses Target of the attack: Host name/IP address (Note: Target of the attack should not be listed for incidents involving personal data)

Once the CISO has determined that an incident has occurred, the CISO will activate this procedure immediately and assemble the SIRT team.

7.2. Severity Assessment

The severity of an incident is a subjective measure of its impact on, or threat to, the operation or integrity of Ex Libris cloud services and its customers' data. It determines the priority for handling the incident, and the timing and extent of the response.

The following factors are considered in determining the severity of an incident:

A. **Magnitude of service disruption** – How many systems or institutions does it affect?

B. **Probability of propagation** – How likely is it that the malware or negative impact will spread or propagate to other systems?

C. **Release or compromise of personal data** – Was confidential personal data compromised?

D. **Remedial actions** – What kind of actions and urgency are required?

Three levels of incident severity will be used to guide incident response: high, medium and low

Severity	Symptoms
High	A. Network or system outage with significant impact on the user population or operation of Ex Libris cloud services. B. High probability of propagation. C. Probable or actual release or compromise of personal data D. Requires immediate remedial action to prevent further compromise of data and adverse impact on network or other systems.
Medium	A. Some adverse impact on the operation of Ex Libris cloud services. B. Adverse effects are localized or contained, or minimal risk of propagation. C. No apparent release or compromise of personal data. D. Remedial but not immediate action is required.
Low	A. Minimal impact on small segment of user population or operation of Ex Libris cloud services. B. Completely localized, with few individuals affected, and presenting little or no risk to other systems. C. No loss or compromise of personal data. D. Remedial action is required.

Note: An incident severity classification may change based on subsequent events or greater knowledge of what happened during the incident.

7.3. Notification/Communication

SIRT Lead will take action to notify the appropriate internal and external parties, as necessary.

Internal Notification (within Ex Libris)

- SIRT Lead will issue or direct all internal communications.
- SIRT Lead will notify Ex Libris senior management, cloud directors, support directors, and 24x7 HUB of the incident and provide ongoing status reports.

External Notification

- In the case of an incident with a severity category of "high," the affected customer(s) will be notified as soon as is reasonably practicable, but no later than twenty four (24) hours after Ex Libris becomes aware of the high security incident.
- The notification shall include, to the extent possible:
    - Incident timeline (date/time that the incident was discovered)
    - The nature of the security incident (network attack, worm/Trojan, etc.)
    - Description of the incident (how it was detected, what occurred)
- In the case of a breach of personal data, the external notification will be handled according to the "procedure for handling notification of personal data breach"(see section 8)
- After initial notification, Ex Libris will keep the affected customer(s) updated at periodic intervals on the status of the incident investigation.
- The affected customer(s) shall receive an incident report, including the root cause analysis results, corrective measures implemented by Ex Libris, and any measures to be taken by the customer (s) to minimize potential damages. Such reports will be provided promptly, but no later than fifteen (15) days after Ex Libris' discovery of the incident.
- Any information Ex Libris provides to the affected customer(s) regarding the security incident is confidential information of Ex Libris and shall be labeled and treated as such.

7.4. Containment

The SIRT will determine and execute the appropriate activities and processes required to quickly contain and minimize the immediate impact on Ex Libris cloud services and Ex Libris' customers.

Containment activities are designed with the following primary objectives:

- Counteract the immediate threat
- Prevent propagation or expansion of the incident
- Prevent further damage to the compromised system and/or data
- Restrict knowledge of the incident to authorized personnel
- Preserve information relevant to the incident

Incident containment activities in a case of unauthorized access include, but are not restricted to, the following:

A. Containment Activities - Unauthorized Access Activities that may be required to contain the threat presented to systems to which unauthorized access may have occurred
A1. Disconnect the system or hosts from the network or access to other systems
A2. Isolate the affected IP address from the network
A3. Where possible, capture and preserve system, host, and application logs, network flows for review
A4. Disable the affected application(s)
A5. Discontinue or disable remote access
A6. Stop services or close ports that are contributing to the incident
A7. Power off the host(s), if unable to otherwise isolate
A8. Notify SIRT of status and any action taken

7.5. Corrective Measures

After the situation is contained, the SIRT moves toward remediating any damage caused by the security incident and identifying the root cause.

Corrective measures are designed with the primary objectives of:

- Securing the Ex Libris cloud environment
- Restoring the Ex Libris cloud environment to its normal state

Corrective activities in a case of unauthorized access include, but are not restricted to, the following:

A. Corrective Measures – Unauthorized Access Activities that may be required to return conditions from unauthorized access to a normal and secure processing state
A1. Change passwords/passphrases on all local user and administrator accounts or otherwise disable the accounts as appropriate
A2. Change passwords/passphrases for all administrator accounts where the account uses the same password/passphrase across multiple appliances or systems (servers, firewalls, routers)
A3. Rebuild systems to a secure state
A4. Restore systems with data known to be of high integrity
A5. Modify access control lists as deemed appropriate
A6. Implement IP-range filtering as deemed appropriate
A7. Modify/implement firewall rule sets as deemed appropriate
A8. Make all personnel “security aware”
A9. Monitor/scan systems to ensure problems have been resolved
A10. Notify SIRT of status and any action taken

7.6. Incident Closure

All incident activities, from receipt of the initial report through Lessons Learned Review, are to be documented. The SIRT Lead is responsible for ensuring that all events are recorded, assembling these records in preparation for, and performance of, the Lessons Learned Review, and ensuring all records are preserved for review. SIRT members may be employed in these efforts.

General Overview of the Incident
Summary of the incident providing a general description of events, approximate timelines, parties involved, resolution of the incident, external notifications required, and recommendations for prevention and remediation.

Detailed Review of the Incident
Description of incident events, indicating specific timelines, personnel involved, hours spent on various activities, impact on customers and user communities (for example, system not available, business continuity issues), ensuing discussions, decisions and assignments made, problems encountered, successful and unsuccessful activities, customer notifications required or recommended (including updates to the 'system status' portal), steps taken for containment and remediation, recommendations for prevention and remediation (short-term and long-term), identification of policy and procedure gaps, results of post-incident review.

Retention
All relevant documentation will be archived by the SIRT Lead in a central repository for a period of time in accordance with Ex Libris' current practices at that time. Access to the documentation and repository is typically restricted to SIRT membership and Ex Libris cloud managers.

7.7. Lessons Learned Review

The SIRT Lead will host a Lessons Learned Review after each medium severity and high severity incident has been resolved. This discussion should be scheduled within 2-3 weeks of the incident's remediation. The review is an examination of the incident and all related activities and events. All activities performed relevant to the incident should be reviewed with an eye toward improving the overall incident response process.

The SIRT's recommendations on changes to policy, process, safeguards, etc., serve both as input to and a by-product of this review. "Fix the problem, not the blame" is the focus of this activity. All discussion, recommendations, and assignments are to be documented for distribution to the Ex Libris cloud operation and engineering groups and follow-up by the SIRT Lead. All records and documents will be audited by an ISO auditor annually as part of the ISO-27001 certification process.

7.8. Post-Incident Report

- Security incidents with a severity category of "high" require completion of a post-incident report (in addition, the COO may request one for any security incident).
- The CISO will be responsible for completing the post-incident report.
- The report should contain a high-level description of the incident and its scope, the impact on Ex Libris cloud services and customers, actions taken to prevent further occurrences, and recommendations for further action
- The COO will review any recommendations in the report and determine additional follow-up actions.
- Post-incident reports must be submitted to the COO, be marked as confidential, and use the form specified in Appendix 1.

8) Procedure for Handling Notification of Personal Data Breach

Incidents suspected or known to involve confidential personal data have special procedures in addition to the normal incident handling procedures outlined in this document.

8.1. Executive Incident Management Team (EIMT)

The **Executive Incident Management Team** (**EIMT**) oversees the handling of security incidents involving personal data (i.e., **Personally Identifiable Information" - PII**). An EIMT may also oversee the response to other high-severity incidents, but the primary purpose is to deal with incidents involving personal data. The purpose of the EIMT is to provide executive guidance to the response process: a) to insure an appropriate, timely, and legal response, b) to make decisions related to the incident, and c) to notify appropriate parties. The team consists of:

1) Ex Libris Chief Operating Officer (COO)
2) Head of affected product Business Unit (URD or URM)
3) Ex Libris General Counsel
4) Representative from Product Management teams

8.2. Breach of Personal Data Procedure

1) If the SIRT determines that personal data has been or may have been breached, the SIRT will immediately notify the COO.
2) The SIRT will oversee additional analysis to gather as much information as possible about what happened, being sure to properly protect evidence.
3) If after analysis the COO and SIRT have confirmed that personal data was not breached, no further special action is required and normal incident response procedures may continue. However, the security of the affected system should be carefully assessed.
4) If the analysis confirms that personal data was breached, the COO will convene the EIMT as quickly as possible.
5) The EMIT will oversee the response, addressing the following issues:
    - Determine which customers need to be notified, how soon they should be notified, and the appropriate method for notification
    - Determine the exact scope of the personal data breach (which individuals were affected, what data was compromised, etc.)
    - Provide affected customer(s) with a description of the breach, the type of data that was the subject of the breach, and other information customer(s) may reasonably request concerning the affected individuals.
    - Assist the affected customer(s) in handling any required notifications to third parties (such as content of public statements, notice to affected individuals, regulators, or others as required by law or regulation)

Appendix 1- Post-Incident Report

Incident Salesforce ID Number: YYYYYYY

Incident Severity:

Incident Title:

Incident Manager (name, title, e-mail, phone):

Date of Initial Suspicious/Malicious Activity:

Date Incident Reported:

Date Incident Fully Contained:

Post-Incident Review Session:

Date:

Participants:

Date Incident Response Completed:

Post-Incident Report Submitted by (name, title, e-mail, phone):

Post-Incident Report distributed to:

Date Post-Incident Report Submitted:

Incident Overview:

Provide a general overview of what happened, indicating how the security incident occurred and the scope of the incident (for example, who was affected, what systems were compromised, the dates of major milestones, etc.). Detailed information, such as a timeline, may be added to the end of the report as appendices.

Incident Detection:

Briefly describe how the incident was first discovered (when, how, and by whom).

Incident Containment & Corrective Measures:

Describe how the incident was contained (prevented from spreading and/or doing further damage) and eradicated (removed from infected hosts). Also describe recovery activities.

Incident Notification
If the incident involved the breach of, or suspected breach of personal data that requires notification, describe how and when the affected customers were notified.

Incident Follow-Up
Identify steps taken to prevent future incidents, lessons learned, and any other recommendations resulting from the incident and the post-incident review session.

A. Steps Taken to Prevent Future Incidents
    i.

B. Lessons Learned
    i. .

C. Other Recommendations
    i.

Appendices
Attach any other relevant information about the incident that should be archived.