Ex Libris Security And Privacy Incident Response Policy

Version 2.0

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.

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.

Compliance

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

Policy Review and Update

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

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
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
- Privacy and Regulation Officer & DPO
- 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
- Determine what type of incident has occurred: security, privacy or both security and privacy
- 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

Security and Privacy 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.

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.

If a data breach has occurred, make sure to complete the documentation in the Event Management Kit.
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:

<table>
<thead>
<tr>
<th>Information to Be Documented</th>
<th>Description/Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reference</td>
<td>Use the assigned Salesforce case number</td>
</tr>
<tr>
<td>Type of incident</td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>• Compromised System</td>
</tr>
<tr>
<td></td>
<td>• Compromised User Credentials</td>
</tr>
<tr>
<td></td>
<td>• Network Attacks (DOS, Scanning, Sniffing)</td>
</tr>
<tr>
<td></td>
<td>• Malware (Viruses, Worms, Trojans)</td>
</tr>
<tr>
<td></td>
<td>• Lost Equipment/Theft</td>
</tr>
<tr>
<td></td>
<td>• Physical Break-in</td>
</tr>
<tr>
<td></td>
<td>• Social Engineering (Phishing)</td>
</tr>
<tr>
<td></td>
<td>• Policy Violation</td>
</tr>
<tr>
<td></td>
<td>• Data Leakage</td>
</tr>
<tr>
<td>Incident timeline</td>
<td>Date/time that the incident was discovered</td>
</tr>
<tr>
<td></td>
<td>Date/time that the incident was reported</td>
</tr>
<tr>
<td></td>
<td>Date/time that the incident occurred (if known)</td>
</tr>
<tr>
<td>Who or what reported the incident</td>
<td>Contact information for the incident reporter: full name, affiliation, organizational, email address, phone number, and location.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Incident contact information</td>
<td>List contact information for all parties involved in the incident.</td>
</tr>
</tbody>
</table>
Information to Be Documented

<table>
<thead>
<tr>
<th>Description/Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include as much information as possible, such as:</td>
</tr>
<tr>
<td>• Description of the incident (how it was detected, what occurred)</td>
</tr>
<tr>
<td>• Description of the affected resources</td>
</tr>
<tr>
<td>• Description of the affected organizations</td>
</tr>
<tr>
<td>• Estimated technical impact of the incident (i.e., data deleted, system crashed, application unavailable)</td>
</tr>
<tr>
<td>• Summary of response actions performed</td>
</tr>
<tr>
<td>• Other organizations contacted</td>
</tr>
<tr>
<td>• Cause of the incident, if known (misconfigured app, unpatched host, etc.)</td>
</tr>
<tr>
<td>• List of evidence gathered</td>
</tr>
<tr>
<td>• Official Common Vulnerabilities and Exposures (CVE®)</td>
</tr>
<tr>
<td>• Description of how to reproduce the exploit</td>
</tr>
</tbody>
</table>

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.

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 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

<table>
<thead>
<tr>
<th>Severity</th>
<th>Symptoms</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>A. Network or system outage with significant impact on the user population or operation of Ex Libris cloud services.</td>
</tr>
<tr>
<td></td>
<td>B. High probability of propagation.</td>
</tr>
<tr>
<td></td>
<td>C. Probable or actual release or compromise of personal data</td>
</tr>
<tr>
<td></td>
<td>D. Requires immediate remedial action to prevent further compromise of data and adverse impact on network or other systems.</td>
</tr>
<tr>
<td>Severity</td>
<td>Symptoms</td>
</tr>
<tr>
<td>----------</td>
<td>----------</td>
</tr>
</tbody>
</table>
| 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.

**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)
  - Data breach notifications will include the completion of the Data Breach forms found in Appendix 2 and Appendix 3.
  - Where appropriate

- 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.

**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:

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

**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**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A1.</td>
<td>Change passwords/passphrases on all local user and administrator accounts or otherwise disable the accounts as appropriate</td>
</tr>
<tr>
<td>A2.</td>
<td>Change passwords/passphrases for all administrator accounts where the account uses the same password/passphrase across multiple appliances or systems (servers, firewalls, routers)</td>
</tr>
<tr>
<td>A3.</td>
<td>Rebuild systems to a secure state</td>
</tr>
<tr>
<td>A4.</td>
<td>Restore systems with data known to be of high integrity</td>
</tr>
<tr>
<td>A5.</td>
<td>Modify access control lists as deemed appropriate</td>
</tr>
<tr>
<td>A6.</td>
<td>Implement IP-range filtering as deemed appropriate</td>
</tr>
<tr>
<td>A7.</td>
<td>Modify/implement firewall rule sets as deemed appropriate</td>
</tr>
<tr>
<td>A8.</td>
<td>Make all personnel &quot;security aware&quot;</td>
</tr>
<tr>
<td>A9.</td>
<td>Monitor/scan systems to ensure problems have been resolved</td>
</tr>
<tr>
<td>A10.</td>
<td>Notify SIRT of status and any action taken</td>
</tr>
</tbody>
</table>

### 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.

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.

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.

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.

Executive Incident Management Team (EIMT)
The Executive Incident Management Team (EIMT) oversees the handling of security incidents involving personal data. 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. Ex Libris Data Protection Officer
5. Representative from Product Management teams

**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 EIMT 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

B. Lessons Learned

C. Other Recommendations

**Appendices**

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

---

**Appendix 2- DATA BREACH NOTIFICATION FORM TO CUSTOMERS AND DATA SUBJECT**

From: Ex Libris
To: [Affected data subject name and address - Customer Name]

Sent by:
• Email
• Sales Force
• Phone
• Other

Dear customer, we regret to inform you that on [date] we have discovered that we have been the subject of a personal data breach.

As a result of the above mentioned personal data breach, the personal data concerning you might have been:
• Disclosed
• Destroyed
• Lost
• Modified
• Accessed
• Other [please specify other possible results] by unauthorized persons.

The following measures have been taken/will be taken to address the data breach:
[list all the measures taken such as: we have moved the data base to a secure location, we have reviewed and strengthened the security measures; we have encrypted our data bases, etc]

If you have any questions or concerns regarding to the data breach, you can contact our Privacy and Regulatin Officer & DPO, Ellen Amsel by email at privacy@exlibrisgroup.com, or by post at Bldg. 9, Malcha Technological Park Jerusalem, Israel 9695809

Appendix 3 - DATA BREACH NOTIFICATION FORM TO THE SUPERVISORY AUTHORITY

From: Ex Libris
To: [name and address of the Supervisory authority]
Sent by:
• Post
• Email
• Fax
Please be informed that on [date] we suffered a data breach that consisted of:
[Please fill in with the data of the occurrence of the data breach, Insert details of the nature of the data breach and a description].

Following the data breach, the following personal data were affected: [e.g. names, contact details, accounts, etc].

We estimate that around [estimated] data subjects and [estimated] records were affected by the data breach.

We believe that the personal data breach might have the following consequences:
[list all possible consequences such as: you might be subject to unsolicited emails; you might be subject to phishing attempts; you might be subject to fraud attempts, etc]

The following measures have been taken/will be taken to address the data breach:
[list all the measures taken such as: we have moved the data base to a secure location, we have reviewed and strengthened the security measures; we have encrypted our data bases, etc].

If you have any questions or concerns regarding to the data breach, you can contact our Privacy and Regulation Officer & DPO, Ellen Amsel by email at privacy@exlibrisgroup.com, or by post at Bldg. 9, Malcha Technological Park Jerusalem, Israel 9695809
## Revision Control

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Nature of Change</th>
<th>Date Approved</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Initial version</td>
<td>Apr 21, 2013</td>
</tr>
<tr>
<td>1.1</td>
<td>Updated – Tomer S</td>
<td>May 6, 2014</td>
</tr>
<tr>
<td>1.2</td>
<td>Updated – Tomer S</td>
<td>Apr 19, 2015</td>
</tr>
<tr>
<td>1.3</td>
<td>Review and Update- Tomer S</td>
<td>Feb 4, 2016</td>
</tr>
<tr>
<td>1.4</td>
<td>Review and Update- Tomer S</td>
<td>Jul 13, 2017</td>
</tr>
<tr>
<td>2.0</td>
<td>Review and Update- Tomer S</td>
<td>Apr 26, 2018</td>
</tr>
</tbody>
</table>

## 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.