# Ex Libris Security And Privacy Incident Response

Version 2.7

## Purpose and Scope

The purpose is to ensure that Ex Libris reacts appropriately to any actual or suspected security or privacy event regarding Ex Libris systems and/or data and that all activities are documented for future reference. This establishes responsibility and accountability and defines the steps required to ensure that security incidents are identified, contained, investigated, remedied, communicated, and documented.

This applies to all systems, personnel, and data at Ex Libris.

## Statement

Management responsibilities and processes will be established to ensure a quick, effective, and orderly response to information security and/or privacy incidents. All activities pertaining to the incident will be documented in a Service Now ticket.

## 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.  examples include:

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

***Event Management Kit*** – internal use only document for recording details of an event.

***SIRT –*** Security Incident Response Team

***CISO –*** Chief Information Security Officer

## Responsibilities

## Security Incident Response Team (SIRT)

The SIRT consists of:

- Senior Vice President & Chief Information Security Officer (CISO) - Team Lead
- Chief Information Officer
- Senior Vice President, Chief Compliance & Privacy Officer VP Product Management
- VP Platform and Tech
- Vice President, Infrastructure Engineering
- Vice President, Product Engineering
- President, Academia & Government
- Senior Director, Privacy
- Senior Director, Infrastructure Engineering
- Director, Infrastructure Engineering
- Director, Cyber Security
- Technical Support Manager
- Cloud Operation Group (COG) Manager
- Cloud Engineering Group (CEG) Manager
- 24 x 7 HUB Manager
- Global Support Organization (GSO) Director

Responsibilities of the SIRT include:

- Coordinating and overseeing the response to incidents in accordance with the requirements of the Security Policy and Regulatory Laws
- Minimizing the potential negative impact on Ex Libris and Ex Libris' customers resulting from such incidents
- Determining what type of incident has occurred: security, privacy or both security and privacy
- Repairing, or coordinating the repair of, damage caused by the incident
- Restoring services to a normalized and a secure state of operation
- Preserving evidence of the incident, as appropriate
- Providing clear and timely communication to all interested parties
- Taking proactive steps to prevent future incidents

# Security and Privacy Incident Response Procedure

Security and privacy incident response includes:

- Reporting the initial information regarding how the incident was identified.
- Collecting the information around the event to understand what has happened and the impact.
- Assessing the event to understand the severity.
- Communicating about the event, which includes:
  - Communication within the immediate event team.
  - Communication within the company, as appropriate.

    - Communication with customers, as appropriate.
- Containing/limiting the current event
- Taking corrective action
- Ensuring that complete documentation is available during and after the event.
- Documenting the Root Cause of the event
- Incident closure
- Lessons learned review

## Incident Identification

A privacy or security incident is initiated when:

- An employee contacts the Information Security Office
- A customer notifies Ex Libris of a security issue
- An alert is created from the Security Information Event Management (SIEM) system

An incident begins when a security or privacy incident is reported to the Chief Information Security Officer, the Chief Privacy and Compliance Officer, or the VP of Infrastructure Engineering. This report could come from an employee, an automated system diagnostic, a customer, or other means.

Customers usually contact us through Salesforce, but can also contact the HUB directly. When the customer contacts us regarding a system disruption, the incident will be escalated to the HUB immediately and will include information regarding the disruption.

## Documenting the Incident Initially

Based on the information collected below, an immediate determination will be made by the CISO or event manager**. If the event involves customer data notify the Chief Privacy and Compliance Officer immediately**.

Once an incident is identified, document the following information in an information system.

| Information | Description |
|---|---|
| Customer data affected? | Yes/No (required) |
| Source | Source of the complaint/issue (e.g., Salesforce ticket, email, individual).<br>Include the following information:<br>Contact information for the incident reporter: Full name, affiliation, organization, e-mail address, phone number and location.<br>If an automated system reported the event: Name of software/product, 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 | Description |
|---|---|
| Incident timeline | Date/time that the incident was discovered<br>Date/time that the incident was reported<br>Date/time that the incident occurred (if known) |
| Type of incident | Examples:<br>• Compromised system<br>• Compromised user credentials<br>• Network attacks (DOS, scanning, sniffing)<br>• Malware (viruses, worms, trojans)<br>• Lost equipment/theft<br>• Physical break-in<br>• Social engineering<br>• Policy violation<br>• Unauthorized access to customer data |
| Detailed description of the incident | • System(s) or product(s) affected<br>• Description of incident<br>• Affected resources and organizations<br>• Estimated technical impact of the incident (i.e., data deleted, system crashed, application unavailable)<br>• Initial actions taken<br>• Cause of incident if known<br>• List of evidence gathered<br>• Official Common Vulnerabilities (CVE)<br>• Individuals contacted |
| Identification of the host(s) | • Source of the incident: List of sources' host names/IP addresses<br>• Target of the attack: Host name/IP address (Note: the target of the attack should not be listed for the incidents involving personal data) |
| Communication | • Internal – Ex Libris only<br>• External – customers or other parties |
| Does this incident require notification within 72 hours? | Yes/No (required) |
| Customer data affected? | Yes/No (required) |

## Severity Assessment

An incident must be assessed to understand the severity and impact of the event. The following factors should be considered:

- Personal information – was personal information affected? This can be customer or employee information.
- Service disruption – did the event disrupt service, and if so, who/what was affected?
- Has the event been stopped or contained, or is it still on-going?
- What is the urgency?

Incident severity will be determined as either high, medium or low. In general, use the following:

| Severity | Symptoms |
|---|---|
| High | Requires immediate remedial action to prevent further compromise of data and adverse impact on network or other systems.<br>1. Network of system outage with significant impact on the user population or operation of Ex Libris cloud services.<br>2. High probability of propagation.<br>3. Probable or actual release or compromise of personal data.<br>4. Requires immediate remedial action to prevent further compromise of data and adverse impact on network or other systems. |
| Medium | Some adverse impact on the operation of Ex Libris.<br>1. Adverse effects are localized or contained, or minimal risk of propagation.<br>2. No apparent release or compromise of personal data.<br>3. Remedial but not immediate action is required. |
| Low | Localized with little or no risk to other systems.<br>1. Minimal impact on small segment of user population or operation of Ex Libris cloud services.<br>2. Completely localized with few individuals affected and presenting little or no risk to other system.<br>3. No loss or compromise of personal data.<br>4. Remedial action is required. |

## 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 Senior Management, Cloud Directors, Support Directors, and 24x7 HUB of the incident and provide ongoing status reports.
- Where applicable, SIRT Lead will notify employees and provide on-going status reports.

**External Notification**

- Where a Data Processing Agreement applies and a confirmed personal data breach occurs, Clarivate will provide notification within 48 hours, or otherwise in accordance with applicable law.
- For all incidents where external notification is necessary, the notification will include:
  - Incident Description (i.e., how it was detected, what occurred, type of security incident(e.g., network attack, worm, phishing) )
  - Event Timeline / Chain of Events (e.g., date and time that the problem occurred, that the incident was discovered, that the problem was corrected, etc.)
  - Root Cause Analysis
  - Identified Gaps
  - Action Performed and Preventative Measures
  - Lessons Learned
- For personal data breaches, refer to Procedure for Personal Data Breach.
- Once the incident is resolved and documented, if appropriate, a report will be sent to the affected external party describing the root cause analysis results, corrective measures implemented, and any additional pertinent information.

## Containment

The objective is to prevent the incident from continuing. This is accomplished by:

- Isolating the incident to prevent it from spreading further.
- Putting measures in place to stop the immediate threat.
- Preventing further damage to the compromised system and/or data.

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

1. Disconnect the system or hosts from the network or access other system.
2. Isolate the affected IP address from the network.
3. Where possible, capture and preserve system, host, and application logs, network flows for review.
4. Disable the affected application(s).
5. Discontinue or disable remote access.
6. Stop services or close ports that are contributing to the incident.
7. Power off the host(s), if unable to otherwise isolate.
8. Notify SIRT of statues and any action take.

*Note: Information pertaining to the incident should be kept confidential until the incident is resolved, at which point the classification of the information will be reconsidered.*

## Corrective Measures

After the incident is contained, a plan should be developed and implemented to correct the cause of the incident. This is accomplished by:

- Identifying the root cause of the incident
- Taking the necessary actions to prevent the incident from recurring
- 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:

1. Change passwords/passphrases on all local user and administrator accounts or otherwise disable the accounts as appropriate.
2. Change passwords/passphrases for all administrator accounts where the account uses the same password/ passphrase across multiple appliances or systems (servers, firewalls, routers).
3. Rebuild systems to a secure state.
4. Restore systems with data known to be of high integrity.
5. Modify access control lists as deemed appropriate.
6. Implement IP-range filtering as deemed appropriate.
7. Modify/implement firewall rule sets as deemed appropriate.
8. Make all personnel “security aware”.
9. Monitor/scan systems to ensure problems have been resolved.
10. Notify SIRT of status and any action taken.

## Lessons Learned Review

After the incident has been managed and corrective actions have been implemented, a review of lessons learned will be performed within a one week period.

## Incident Closure

All incident activities, from receipt of the initial report through Lessons Learned Review, will be documented in a ticketing system. The SIRT Lead will ensure that all the activities regarding the incident are recorded and will organize the lessons learned review.

# Procedure for Handling Notification of Personal Data Breach

- When it is determined that personal data is involved, the Chief Privacy and Compliance Officer will immediately notify the President Academia and Government, the Chief Information Officer, the Chief Information Security Officer, Chief Risk Officer and General Counsel.
  - If further analysis confirms that personal data was not breached, no additional special actions are required. Normal incident response process should continue.
- When the analysis identifies what personal data was breached, the Chief Privacy and Compliance officer will convene a meeting immediately to:
  - Determine the exact scope of the personal data breach (which individuals were affected and what data was compromised)
  - Determine which customers need to be notified and the method for notification.
    - Provide affected customer(s) with a description of the breach.
    - Where appropriate, assist the customer(s) as needed.

· When customer data has been breached, the customer will be called personally to notify them.

- Document in detail in a ticketing system what actions were taken, including who was notified.

## Notification for a Personal Data Breach

All notifications regarding a personal data breach will be developed in conjunction with Legal.

# Compliance

Failure to comply with this will result in disciplinary action up to and including termination of employment.

# 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**
- **Phone**

---

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

---

**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, We have designated a Group Data Protection Officer who serves for the group of companies. You can contact our Group Data Protection Officer at privacy@exlibrisgroup.com. For more information please see our Privacy Policy.

## 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**
- **Other**

---

**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, We have designated a Group Data Protection Officer who serves for the group of companies. You can contact our Group Data Protection Officer at privacy@exlibrisgroup.com. For more information please see our Privacy Policy.

### Record of Changes

| Type of Information | Document Data |
|---|---|
| Document Title: | Ex Libris Security and Privacy Incident Response |
| Document Owner: | Eddie Lavian - Cyber Security Engineer |
| Approved by: | Tomer Shemesh - Senior Director, Information Security |
| Issued: | April 21, 2013 |
| Reviewed & Revised: | November 28, 2024 |

### Revision Control

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

| Version Number | Nature of Change | Date Approved |
|---|---|---|
| 2.1 | Review and Update- Tomer S | Jul 17, 2019 |
| 2.2 | Review and Update- Tomer S | Nov 05, 2020 |
| 2.3 | Review and Update- Tomer S | Aug 25, 2021 |
| 2.4 | Review and Update- Tomer S | Jul 11, 2022 |
| 2.5 | Review and Update -Tomer S | Nov 23, 2023 |
| 2.6 | Review and Update - Tomer S | Nov 28, 2024 |
| 2.7 | Review and Update - Tomer S | Nov 23, 2025 |

**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