Security and Privacy

General

Within the cloud environment, what type of file or application auditing/logging is available?

At the cloud infrastructure level, Ex Libris collects and archives system logs and retains all records of access by Ex Libris cloud personnel. Since the service is a multi-tenant cloud service, these security/system logs include data related to all customers sharing the cloud environment and as such can't be provided. The application includes an audit trail that could be used by the university to identify all access/logins to the customer data (customer institution) - this audit trail includes access records for all the logins of the customer staff and access records of Ex Libris support personnel. The audit trail report could be generated by the customer without the help of Ex Libris.

On a daily basis, the Security Officer reviews the daily reports of suspicious activity (e.g., failed authentication attempts).

Ex Libris' NOC (Hub) provides 24x7 logging and monitoring for all logical network access to customer data and information asset usage and is audited by the Ex Libris Security Officer. Ex Libris monitoring consists of multi-layered, fully redundant systems that monitor the services inside and outside the Data Center to validate that services are running at the highest performance levels.

Data Centers

In what operating environment is Alma managed?

Ex Libris works with a number of vendors in their data centers around the world:

- United States (Equinix) data center
- United States (Cyxtera) data center
- Canada (Cyxtera) data center
- Europe (Equinix) data center
- Europe (Digital Realty) data center
- China (21vianet) data center
- Singapore (Equinix) data center
- Australia (Equinix) data center

All of the servers, switches, storage etc., are owned and maintained by Ex Libris cloud personnel. As a multi-tenant solution, the infrastructure is shared among multiple customers. The Ex Libris Cloud Data Center utilizes 1G bandwidth as its backbone, and works with multiple ISP vendors at every point in time.

Ex Libris implements a multi-tiered security audit on different levels: security checks and manual code reviews daily,

security architecture reviews monthly, static application security vulnerability assessment scans quarterly, as well as third-party patching on a quarterly basis and an annual scan of network vulnerabilities. The ISO 27001 certification that Ex Libris passed successfully includes annual external audits to validate that all security measures and mitigations are in place.

Ex Libris also conducts an annual security penetration test with an external security company which includes at least the OWASP Top 10 and SANS Top 25 security vulnerabilities, which validates that all security measures are in place.

About once per year, the Ex Libris data centers and applications undergo an audit. For example, the Ex Libris data facilities recently went through an in-depth audit of their control objectives and control activities and a SSAE16 SOC1 audit report was issued. The company's ISO 27001 audit covered cloud services, development, QA, support and professional services processes, including internal risk assessment process required by ISO Certification.

See An overview of the Ex Libris cloud and datacenter operations and A short virtual tour for more details.

Privacy

How does Alma provide security and privacy safeguards?

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:

- Ex Libris Chief Operating Officer (COO)
- Head of affected product Business Unit
- Ex Libris General Counsel
- Representative from Product Management teams

If the SIRT determines that personal data has been or may have been breached, the SIRT will immediately notify the COO. The SIRT will oversee additional analysis to gather as much information as possible about what happened, being sure to properly protect evidence.

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.

If the analysis confirms that personal data was breached, the COO will convene the EIMT as quickly as possible. 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.

Ex Libris has developed extended authorization controls to protect customer data with role-based access control (RBAC):

- Staff members must authenticate prior to accessing Alma
- Each staff member has privileges and access to data limited to his/her role
- Only authorized staff members have access to view and edit patron data
- Alma's browser sessions are encrypted using TLS.

To what extent does Alma comply with data privacy regulations such as FERPA?

Alma conforms to FERPA guidelines by providing multi-tier access control based on the security industry's best practices. Such controls consist of (but are not limited to):

- Staff member authentication prior to accessing Alma
- Each staff has privileges and access to data according to his/her role
- Only authorized staff members have access to patron data, to view and edit
- Alma's browser sessions are encrypted using TLS
- Sensitive Patron information is encrypted

Alma maintains an audit trail of access to patron data that has been exported. This information may be used in conjunction with the institutions' written approvals by students and/or their parents to track any export of patron's data outside of Alma

In terms of payment standards such as the Payment Card Industry Data Security Standard (PCI-DSS), Alma does not maintain credit card information and as such this regulation does not apply.

Will a customer's application(s)/data co-exist with that of other customers?

Yes - Alma is a multi-tenant cloud solution. As a multi-tenant cloud service we enforces strict data isolation to all layers of the application: user-interface branding isolation, storage isolation, and SFTP-level isolation. In addition, our cloud service makes use of Oracle Virtual Private Database (VPD) in order to provide complete data isolation also at the database level. Finally the security penetration testing performed by an external security company validates that all isolations and segregations are in place.

How is segregation of data between customers achieved?

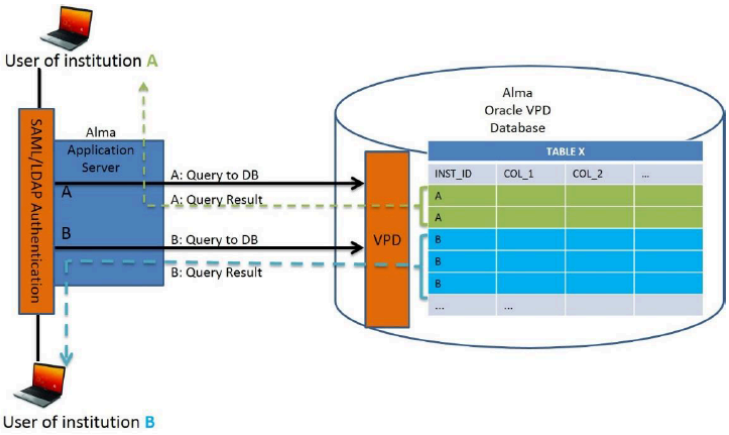
Alma utilizes Oracle Virtual Private Database capabilities in order to provide complete segregation between the different institutions that are served by Alma.

The Oracle VPD enables the creation of security policies to control database access at the row and column level. Oracle Virtual Private Database enforces security, to a fine level of granularity, directly on database tables, views, or synonyms. Since the security policies directly attached to these database objects, and the policies are automatically applied whenever a user accesses data, there is no way to bypass security. More on Oracle VPD can be found on the below link: http://docs.oracle.com/cd/B28359_01/network.111/b28531/vpd.htm#CIHHDHGD

As illustrated in the diagram below:

- User is first authenticated through either SAML or LDAP against the institutional authentication system;

- When the application needs a database connection to fulfill the user's request, the application infrastructure allocates a connection and sets its context parameters with the user's institution key, which was validated during the authentication process;
    - There is no other way to set these context parameters within the application which makes the process more secure.
    - The connection values to the database can only be set as part of the authentication process of the user, as a means to further increase security protection.
    - The entire connection is made using a secured communication channel.
- The application server uses the connection values, including the unique institution ID to establish connection to the database on behalf of the user
- The connection is made to the VPD component of the database that that uses the security elements described earlier to guarantee a high level of security and complete segregation between different institutions.



Does the Ex Libris cloud service require access to the university's identity services?

Yes - Ex Libris SaaS service requires the use of authentication through the customer's identity management system, using standard protocols such as LDAP, SAML 2.0 and CAS. Passwords are managed by the customer and are not stored in the SaaS service.

How does the cloud service manage who is granted access to Alma?

Authorization is managed at the application tier (roles are not passed from the university directory). The Alma authorization mechanism is based on the role-based access control (RBAC) model, which supports the segregation of duties. Users can only access functional areas and data that are derived from their roles and privileges.

Security

What version of TLS is supported?

Alma supports TLS1.2. See Transport Security Layer (TLS) Support.

What tools and procedures are there that will prevent and detect unauthorized attempts to access an institution's systems?

A combination of an intrusion detection system (IDS) and intrusion prevention system (IPS) is installed and tracks all illegal activities. The system sends real-time alerts and proactively blocks communication once a suspicious attack is discovered. The system performs various activities on the network: log collection and analysis from the various machines (firewalls, switches, and routers), file integrity checking, and rootkit detection.

What tools and procedures are in place to detect and defend an institution's systems against malware and virus attacks?

To defend against malicious malware, Ex Libris utilizes a leading malware solution. The malware protection system includes virus, spyware and Trojan protections.On an ongoing basis, vulnerabilities are monitored and validated and where appropriate, blocked, to ensure that no false positives will impact the stability and availability of our service. When Ex Libris identifies DOS (denial of service) and DDOS (distributed denial of service) attacks, they are blocked. Security vulnerabilities that are considered high risk or severity are blocked by default. We continue to configure and block attacks at all levels, including at the ISP, on our perimeter firewalls, network devices and intrusion detection/prevention system. Additionally, Ex Libris has a dedicated 24/7 NOC (known as the Hub) that monitors all activities and has documented procedures to handle any security or privacy event, including DOS and DDOS attacks. For any security or privacy event, a root cause analysis is performed afterwards, and based on the lessons learned, additional controls may be implemented throughout the various layers of protection in place as needed.

What tools and procedures are in place to cleanse a hacking or virus attack?

According to the Ex Libris backup policy, we take at least four backup snapshots of the entire data during the day, in addition to a full backup that is also maintained in a remote secured site. Should there be a successful virus attack on our environment, of dedicated anti-malware tools are used to clean our data including the ability to use one of the virus-free backup snapshots that were taken for the recovery of the data to the point right before the virus attack.

What is the frequency of updates for anti-malware library definitions and anti-virus scans?

Anti-malware and anti-virus are updated on an ongoing basis and immediately once an update has been released by the vendors and has been tested in the Ex Libris cloud testing environment prior to deploying to the production environment.

How is media sanitized and disposed when no longer required?

Ex Libris has strict procedures and a policy for handling obsolete removable media based on the NIST standard for clearing and sanitizing data on writable media. These procedures are also applied if a customer decides to terminate the service. Disks and tapes are destroyed once they are no longer needed. CDs that are no longer needed are destroyed by a CD/DVD data crusher or shredder. All storage devices that may need to be used again are cleaned by data wipe software.

Does Ex Libris have written information on security policies?

Yes. These can be viewed at the following online location: http://knowledge.exlibrisgroup.com/Cross-Product/Security/Policies

What security methods/protocols are utilized to protect the overall solution?

Cloud security and confidentiality are top concerns with cloud computing and software-as-a-service (SaaS) architecture. Ex Libris is committed to providing our customers with the most secure and reliable environment, and has developed a multi-tiered security model that covers all aspects of our cloud-based systems. Ex Libris is ISO 27001:2013 certified and our model and controls are based on international protocols and standards, such as ISO/IEC 27001:2013 and ISO/IEC 27002, the standards for an information security management system (ISMS).

The Ex Libris security model defines the security controls applied to address vulnerabilities, as illustrated in the figure below.

Safety Protocols

Alma is designed to safeguard data throughout the data lifecycle including data in transit. Alma utilizes TLS encryption (based on a commercial TLS certificate), which creates an encrypted channel between the client computer and the Web server, and between the application server and the database server. In addition, the customer's personal data stored by Ex Libris will also be encrypted to prevent unauthorized access, and such data can be read only by the application.

Encryption

Encryption and decryption of personal information will be performed in real time so that data at rest is always protected. Ex Libris uses a standard mechanism for handling the encryption keys: all encryption keys are random, and are stored separately from the credential management zone. Encryption keys are never exposed in a clear form, and they are destroyed at the end of their designated period.

Obsolete Data

Ex Libris has strict procedures for handling obsolete data; these procedures are also applied if a customer decides to stop

using Alma. Authorized personnel remove all data from disks and tapes by means of a degausser once the data is no longer needed. CDs that are no longer needed are destroyed by a CD/DVD data crusher or shredder. All storage devices that may need to be used again are cleaned by data wipe software.

Unauthorized Access

Security controls at the Ex Libris data centers are based on standard technologies and follow the industry's best practices. Physical security controls are constructed in such a way as to avoid the effect of single points of failure, and retain the resilience of the computing center.

SSAE16 SOC1 Audit

The Ex Libris data centers received an in-depth audit of the centers' control objectives and control activities, including controls over information technology and all other related processes, resulting in a SSAE16 SOC1 service auditor's report.

Physical Access Control

Physical access to the data center is restricted to personnel with a business need to access the infrastructure. All physical access activities are logged and monitored. Ex Libris visitor access policy requires that all visitors to the data center be approved beforehand, and the approval is for a limited period of time. Visitors must be accompanied by an authorized employee throughout their visit.

Access Control

Ex Libris has well-developed processes to safeguard the privacy and security of library patrons' data. To secure the data, Ex Libris requires the authentication of users who are trying to access the system and authorization when they are using the system.

Authentication

Alma implements a security feature that locks out a user who attempts to log on more than a defined number of times. Alma also enforces strict password rules, which apply to both the operational team members and the application's users. Password rules include aging, length, combination, and reuse enforcement. All passwords are stored encrypted, using a one-way encryption method based on an industry-standard hash algorithm; only the application is able to compare the hashed and entered passwords. Passwords are never exposed by the application or sent by e-mail.

Alma's authentication architecture also supports single sign-on (SSO), which uses the enterprise identity provider authentication system. In this architecture, Alma delegates authentication to the customer's identity provider, whereby a circle of trust is built with the different domains. In this case (depending on the customer's identity provider being used), federation standards (based on the Security Assertions Markup Language [SAML] protocol) are applied.

Since the privacy and confidentiality of our customers' data is our top priority, Ex Libris has developed extended authorization controls. The Alma authorization mechanism is based on the role-based access control (RBAC) model, which supports the segregation of duties. Segregation of duties is applied in order to minimize the risks and possibilities of misusing privileges. Users see only the menus and data that are derived from their roles and privileges. The system is constantly tested to ensure that users do not have multiple privileges that allow them to perform roles that conflict with other roles.

All access control activities produce logs with information to meet auditing requirements and support usage charges. In addition, the access control activities generate notifications to designated library staff to prevent users from setting up rogue accounts or otherwise modifying access entitlements.

Protection of User Data

Alma provides multi-tier access control that is based on security industry best practices.

Access to Alma consists of:

- Staff members must authenticate prior to accessing Alma;
- Each staff member has privileges and access to data limited to his/her role;
- Only authorized staff members have access to view and edit patron data; and
- Alma's browser sessions are encrypted using TLS.

A related capability is the audit trail. Alma maintains an audit trail of access to patron data that has been exported out of Alma. This may be used in conjunction with the institutions' written approvals by students and/or their parents to track any export of patron's data outside of the Alma system.

PCI-DSS compliance is not applicable as Alma stores no credit card information. Alma also stores no health-related data, so HIPAA regulations also are not applicable.

In addition all of Alma's integration interfaces with local institutional systems are secured whether through the use of secured FTP, secured SMTP, Stunnel for self-check machines integrations and all of Alma's APIs are secured.

Does Alma comply with standard security regulations?

Ex Libris solutions comply with Data Protection Act 1998 and Equality Act 2010.

In addition, Ex Libris solutions comply with all applicable laws and regulations including the Freedom of Information Act 2000, Environmental Information Regulations 2004, Copyright, Designs and Patents Act 1988, Health and Safety at Work Act 1974 and National Audit Act 1983.

Ex Libris ensures that it complies with the legal requirements regarding Data Protection, Cloud Security and Accessibility. Cloud security and confidentiality are top concerns with cloud computing and software-as-a-service (SaaS) architecture. Ex Libris is committed to providing our customers with the most secure and reliable environment, and has developed a multi-tiered security model that covers all aspects of our cloud-based systems. Ex Libris is ISO 27001:2013 certified and our model and controls are based on international protocols and standards, such as the above mentioned ISO/IEC 27001:2013 and ISO/IEC 27002, the standards for an information security management system (ISMS). Ex Libris has also earned, ISO 27018:2014 certification. ISO 27018:2014 is a new international data privacy standard for protecting personally identifiable information (PII) in public clouds.

In addition, the use of a data centre in Amsterdam meets the requirements of the EU Safe Harbor directive 95/46/EC.

Ex Libris conforms to accessibility guidelines when possible in terms of the underlying technology used by the solution. Ex Libris' policy is to comply with accessibility regulations, and – in particular – to make end-user facing interfaces as accessible as possible.

All Ex Libris' products and services comply with the requirements of the UK Equality Act. Ex Libris is committed to ensuring that its existing software and planned releases comply with accessibility standards. Alma was developed in line with the WAI guidelines. The application is compliant by applying a high-contrast level of the display, by adjusting the luminosity level of the display, and by applying alternatives to non-accessible methods, such as JavaScript or AJAX components. The application is also compatible with screen readers for the visually impaired. As far as possible, hot keys (keyboard shortcuts) have been defined for functions in the system; this is especially true for circulation functions.

The accessibility of the Primo interface for users has been validated by several rounds of usability studies. The Primo version 4 user interface was designed to comply with leading international accessibility and industry standards: The W3C Web Content Accessibility Guidelines 2.0, level "Double-A" Section 508 of the Rehabilitation Act (29 U.S.C. 794d).

Does security incorporate Software/Service Design Life Cycle?

Ex Libris products follows the Agile System Development Life Cycle (SDLC). This allows Ex Libris to deliver monthly releases and to respond quickly to customer needs in a multi-tenancy cloud-based SaaS environment, including security. Secure coding practices and security awareness are an integral part of the SDLC process.

As part of the Ex Libris development life cycle policy and process, audits are performed by the team leader or the code author. Tests of the code review are done by the Security Officer who performs a security review and vulnerability assessment at least on quarterly basis, in addition to an annual application penetration test that verifies that security measures are in place.

Are employees with access to customer data subject to background checks?

Prior to the employment of new staff by Ex Libris, individuals are subject to vetting and are required to sign confidentiality agreements. Background checks are performed for staff employed in critical roles and who have direct access to customer production data - such as system administrators.

Are employees with access to customer data required to sign a confidentiality agreement?

Prior to the employment of new staff by Ex Libris, individuals are required to sign confidentiality agreements. Additionally, Ex Libris incorporates the philosophy of “least privilege” and “need to know” principles for authentication, security requirements, separation, isolation, segregation, and security measures as part of operating procedures. Ex Libris’ ISO 27001:2013 certification confirms that these security practices are in place.

How does Ex Libris mitigate risk if employee’s services are terminated or suspended?

User permissions are continuously updated and adjusted so that when a user's job no longer involves infrastructure management, the user's console access rights are immediately revoked. This process is enforced for any change or status or employee termination.

Ex Libris realizes that the malicious activities of an insider could have an impact on the confidentiality, integrity, and availability of all types of data and has therefore formulated policies and procedures concerning the hiring of IT administrators or others with system access. Ex Libris defined and implemented security policies and procedures including “least privilege” and “need to know” principles and authentication and security requirements to protect customer information. Ex Libris has also formulated policies and procedures for the ongoing periodic evaluation of the Security Officer or others with system access. Any violation of the policy handled by the Security officer includes revoking permissions to access the system and even an HR hearing, up to employee termination.

How does Ex Libris notify the university in the case of a breach of security?

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

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

Since the privacy and confidentiality of our customers' data is our top priority, Ex Libris has developed extended authorization controls. The Alma authorization mechanism is based on the role-based access control (RBAC) model, which supports the segregation of duties. Segregation of duties is applied in order to minimize the risks and possibilities of misusing privileges. Users see only the menus and data that are derived from their roles and privileges. The system is constantly tested to ensure that users do not have multiple privileges that allow them to perform roles that conflict with other roles.

All access control activities produce logs with information to meet auditing requirements and support usage charges. In addition, the access control activities generate notifications to designated library staff to prevent users from setting up rogue accounts or otherwise modifying access entitlements.

Protection of User Data

Alma provides multi-tier access control that is based on security industry best practices.

Access to Alma consists of:

- Staff members must authenticate prior to accessing Alma;
- Each staff member has privileges and access to data limited to his/her role;

- Only authorized staff members have access to view and edit patron data; and
- Alma's browser sessions are encrypted using TLS.

A related capability is the audit trail. Alma maintains an audit trail of access to patron data that has been exported out of Alma. This may be used in conjunction with the institutions' written approvals by students and/or their parents to track any export of patron's data outside of the Alma system.

PCI-DSS compliance is not applicable as Alma stores no credit card information. Alma also stores no health-related data, so HIPAA regulations also are not applicable.

In addition all of Alma's integration interfaces with local institutional systems are secured whether through the use of secured FTP, secured SMTP, Stunnel for self-check machines integrations and all of Alma's APIs are secured.

Does Ex Libris complete a PCI-DSS/DA v2/v3 audit for Alma?

PCI-DSS compliance is not applicable as Alma does not store or process credit card information.

Does Alma support mail relay for customer notifications?

Alma and Primo use dedicated mail-relay servers in each region.

Ex Libris supports Transport Layer Security (TLS) on the mail-relay servers to deliver mail securely.

Secure SMTP over TLS allows for encrypted messages; TLS uses Public Key Infrastructure (PKI) to encrypt messages from mail server to mail server.

The preferred (default) setup of the Alma email servers involves the use of encrypted transactions. If a customer's email servers support TLS, Ex Libris upgrades the SMTP session to use TLS. If TLS is not supported on the customer's email servers, Ex Libris establishes the session without TLS.

Alma email servers support encrypted emails (TLS) signed with a GoDaddy certificate. If a customer's email servers support TLS, it is recommended that GoDaddy be added as a root certificate authority to the MTA. (Note that when the certificate is not verified, the email is delivered as "untrusted" to the customer.)

Ex Libris strongly recommends that the customer add the IP addresses of Ex Libris' mail-relay servers to the 'Allowed List'.

See also: Technical Requirements for Alma and Discovery Implementation/Mail Relay Gateways

Encryption

See also: ...User Management/Security and Privacy

How does Alma support data transit security?

Alma is designed to safeguard data throughout the data lifecycle, including data in transit. Alma utilizes TLS encryption (based on a commercial TLS certificate), which creates an encrypted channel between the client computer and the Web server, and between the application server and the database server. Encryption channel also covers all Alma communication including Secured FTP, secured SIP communication and secured communication with email servers.

What encryption options are in place?

Alma encrypts patrons' personal information such as email, address, phone, etc. This data is kept encrypted in the database. Ex Libris uses a standard mechanism for handling encryption keys: all encryption keys are random, and are stored separately from the credential management zone. Encryption keys are never exposed in a clear form, and they are destroyed at the end of their designated period. The encrypted data remains as such, as well as in the backups we make to our cloud data.

What method(s) for encryption both at rest and in transit are used?

Ex Libris Alma makes use of the following encryption mechanisms:

- Data in motion: browser to application server connections are https utilizing TLS 1.2 using SHA-1 128 or 256 key and AES 128 or 256. The TLS version and key strength are negotiated upon session establishment, between the server and the browser.
- Data at rest: personal information is kept encrypted using disk encryption using AES-256 encryption. In addition, we are encrypting data in the level of database using Oracle DBMS_CRYPTO mechanism based on AES-256 encryption.
- Backup of the data is made to disk and the encrypted data is kept encrypted in the backup copy.

Is personally identifiable information (PII) encrypted?

Personally identifiable information (PII) is encrypted in-transit and at rest. PII is also encrypted on backups.

What encryption levels does Alma provide?

Committed to providing our customers with the most secure and reliable environment, Ex Libris has developed a multi-tiered security model that covers all aspects of cloud-based Ex Libris systems. The security model and controls are based on renowned international protocols and standards and industry best practices, such as ISO/IEC 27001:2013 and ISO/IEC 27002, the standards for an information security management system (ISMS).

Alma is designed to safeguard data throughout the data lifecycle, including data in transit. Alma utilizes TLS encryption (based on a commercial TLS certificate), which creates an encrypted channel between the client computer and the Web server, and between the application server and the database server. In addition, the customer's personal data stored by Ex Libris will also be encrypted to prevent unauthorized access, and such data can be read only by the application. Ex Libris uses a standard mechanism for handling encryption keys: all encryption keys are random, and are stored separately from the credential management zone.

Ex Libris Alma makes use of the following encryption mechanism and strength:

- Data in motion: browser to application server connections are https utilizing TLS 1.2 using SHA-1 128 or 256 key and AES 128 or 256. The TLS version and key strength are negotiated upon session establishment, between the server and the browser
- Data at rest: personal information is kept encrypted in the database using Oracle DBMS_CRYPTO mechanism for data encryption using AES-256 encryption. Backup of the data is made to disk and the encrypted data is kept encrypted in the backup copy

What unencrypted protocols are in use?

All communications are protected by using secure protocols such as SFTP.

Some protocols work based on unsecured TCP based connections. An example is the SIP2 protocol, commonly used by Self Check machines. For these, the Alma SIP2 server is used with the Stunnel software, which is a free software used to secure traffic running between a TCP client and server. It is designed to work as an TLS encryption wrapper, encrypting the messages using industry-standard crypto libraries (such as OpenTLS) and allowing for secure communication without changing the program running on either side of the TCP connection.

Alma uses Stunnel to secure the communication in the following integrations:

- Self check
- Remote storage facility