SAFARI MONTAGE

SAFARI Montage® Products and Services

Data Security Controls

Thank you for using SAFARI Montage products and services. SAFARI Montage is the leading K-12 Learning Object Repository, Video Streaming Library, IPTV, & Live Media Streaming provider. The system provides an interoperable foundation for a digital learning ecosystem where teachers and students can access procured, created, and curated educational digital resources, create playlists, and integrate items into their LMS.

Whether on-prem or in the cloud, SAFARI Montage endeavors to carefully protect sensitive information in our care, including—and especially—student data.

SAFARI Montage will never sell student data or use it for advertising. We only disclose personally identifiable user data to third parties if necessaryin order to deliver SAFARI Montage products and services to our customers or as required by law. We strive for transparency in the way we collect, use, and disclose data, which we detail in our Products and Services Privacy Policy.

The following security controls provide a window into how we protect our products and services from unauthorized access. While it is impossible to protect against all security threats, we believe our program is robust, reasonable, and appropriate to protect student data in our control.

1. Planning

SAFARI Montage maintains a risk-based, written information security program based on industry recognized administrative, technical, and physical safeguards designed to secure sensitive data collected or accessed by our on-prem and cloud-based solutions. Our cross-functional security team develops, documents, and routinely reviews and updates our security policies and procedures to address critical practice areas such as access control, vendor selection, incident response, and security training.

2. Awareness and Training

We believe that information security awareness and adherence to our policies and procedures is the responsibility of every employee. We ensure that all employees are adequately trained regarding data privacy (such as FERPA, COPPA, and applicable state laws) and security awareness upon hire and on an ongoing basis. Our training includes annual structure training with assessment plus regular unannounced simulated phishing exercises to continually improve our security competence. Individual and organizational training compliance is documented and analyzed in order to identify and mitigate areas of weakness.

3. System and Services Acquisition

SAFARI Montage cloud products leverage Microsoft Azure and Amazon Web Services (AWS) for cloud hosting. The security, privacy, and compliance practices for these industry leaders are available at the Azure Trust Center and AWS Cloud Security.

We adhere to a comprehensive vendor assessment policy and review the information security and continuity practices of all vendors employed in the development and delivery of all of our products and all open- and closed-source software and services undergo cross-functional, security, and legal review.

4. Access Control

SAFARI Montage maintains strict access controls to all systems involved in granting access to student data. Technical support systems are restricted to personnel requiring access to perform their job functions. Two-factor authentication is enabled for remote VPN access, Microsoft 365 email, productivity applications, storage, and cloud services.

Whether utilizing the cloud or on-prem solution, customers maintain complete control over access, authentication, and audit controls.

5. Identification and Authentication

SAFARI Montage maintains strict authentication controls for all systems, including those that provide access to customer systems through privileged technical support methods.

Our solutions anticipate the delegation of user account management and authentication and relegate policy enforcement of access control to a customer-operated facility (such as Active Directory) where the customer manages, for example, logon attempt limits and password complexity.

Passwords are encrypted in data storage locations and password entry fields are obfuscated in user interfaces. User authentication at login occurs using a minimum of 256-bit AES encryption and is secured in transit using HTTPS/TLS 1.0 or higher. All sensitive data is uploaded via secure FTP services and remote access is conducted over SSH.

6. Audit and Accountability

SAFARI Montage maintains logs and records of all employee support access to customer systems through privileged technical support access methods. SAFARI Montage applications log and record notable events, including successful and failed logins, direct logins, remote logins, and system access from third-party LMS, systems, or from permanent links. Audit logs include time, date, user account, details of action, source IP address, and other information relevant to profiling system activities, all of which enables the monitoring, analysis, investigation, and reporting of unauthorized system activity.

Customers maintain control with respect to their internal users and manage any access granted to SAFARI Montage employees for support and maintenance reasons via customer-provided user accounts, including access, authentication, and audit controls.

7. Security Assessment and Authorization

We regularly review federal, vendor, and community technical and security advisories and publications to maintain awareness of new security developments, practices, and potential vulnerabilities requiring assessment and attention.

Internal systems and infrastructure where employees access or handle student data are subjected to standard periodic vulnerability scanning to identify and remedy security issues. Each SAFARI Montage application and OS version is subjected to regular vulnerability scanning to identify and remediate relevant security issues prior to release.

8. Contingency Planning

SAFARI Montage personnel and systems supporting customer-hosted installations have defined contingency plans to provide for continuity of support services in cases of environmental or systems failures.

SAFARI Montage cloud installations leverage a natively redundant Azure or AWS environment for both local and zone redundant operation at all times, ensuring that customer installations continue to experience uninterrupted service in the event of any single site failure.

Contingency planning for customer-hosted, on-prem installations of SAFARI Montage applications is managed by the customer.

9. Incident Response

SAFARI Montage maintains a comprehensive incident response plan, managed by a distinct team of trained individuals, to manage and respond to any actual or suspected security incident or breach in order to investigate, contain, remediate, and promptly notify affected parties of security incidents.

10. Maintenance

All internal system hardware, applications, and operating systems are regularly maintained and any issues are remediated promptly. All activities performed by external personnel are monitored and documented. All new versions of SAFARI Montage applications, OS, and hardware are assessed and updated as required.

11. Media Protection

All cloud-hosted student data is encrypted in transit using SSL and at rest using a minimum of 256-bit AES encryption. Encryption is enabled for all cloud storage accounts as well as data stored on managed OS and data disks using service level or server-side encryption using a minimum of 256-bit AES and is FIPS 140-2 compliant.

All on-prem solution student data is encrypted in transit using SSL and content storage drives are encrypted at rest using a minimum of 256-bit AES encryption.

12. Physical and Environmental Protection

SAFARI Montage physically secures all systems involved in supporting and accessing customer systems. Internal systems are physically secured via least privilege access controls ranging from physical locks and door access key codes to video monitoring and retinal scanning.

For SAFARI Montage cloud installations operating on Azure and AWS platforms, data centers managed by those entities comply with a broad set of international and industry-specific compliance standards and validations, such as NIST SP 800-171, ISO 27001, SOC 1, and SOC 2.

Customers manage physical and environmental security controls for customer-hosted installations.

13. Personnel Security

All employees have signed confidentiality agreements to protect sensitive data that they may access, and employees who visit customer locations for installations, support, and training undergo criminal background checks.

Employee on- and off-boarding processes are structured to ensure that employee access to customer and privileged systems is granted solely on least privilege security needs, adjusted appropriately upon any change of responsibility, and terminated immediately upon separation from the company.

14. Risk Assessment

SAFARI Montage regularly assesses active risks and subjects internal systems to vulnerability scanning to identify and address security risks. Annual external audits of our ERP solution are conducted, including management review and remediation. Open-source software is reviewed to ensure appropriate licensing and security. All vendors undergo a comprehensive internal review to identify potential risk factors and ensure appropriate safeguards are in place.

15. System and Communications Protection

All internal and external logical boundaries are appropriately secured and all inbound traffic is managed on a deny all/explicit allow approach. All SAFARI Montage client traffic is subject to network-level security scanning, intrusion prevention technologies, and endpoint protection. Active measures are employed to detect and block suspicious activity.

16. System and Information Integrity

SAFARI Montage reviews government, vendor, and community technical security advisories and publications on an ongoing basis to maintain awareness of new security developments, practices, and potential vulnerabilities requiring assessment and attention.

Relevant internal systems and infrastructure are subjected to standard periodic vulnerability scanning to identify and remedy any potential security issues.

For additional information regarding SAFARI Montage Data Security Controls, please contact privacy@safarimontage.com.