A-LIGN

A-LIGN.com

Type 2 SOC 3

Prepared for:
Magnolia International, Ltd.

Year:
2026

magnolia

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

February 1, 2025 to January 31, 2026

Table of Contents

SECTION 1

ASSERTION OF MAGNOLIA INTERNATIONAL, LTD. MANAGEMENT

ASSERTION OF MAGNOLIA INTERNATIONAL, LTD. MANAGEMENT

March 13, 2026

We are responsible for designing, implementing, operating, and maintaining effective controls within Magnolia International, Ltd.'s ('Magnolia' or 'the Company') Content Management Software Services System throughout the period February 1, 2025 to January 31, 2026, to provide reasonable assurance that Magnolia's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented below in "Magnolia International, Ltd.'s Description of Its Content Management Software Services System throughout the period February 1, 2025 to January 31, 2026" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period February 1, 2025 to January 31, 2026, to provide reasonable assurance that Magnolia's service commitments and system requirements were achieved based on the trust services criteria. Magnolia's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in "Magnolia International, Ltd.'s Description of Its Content Management Software Services System throughout the period February 1, 2025 to January 31, 2026."

Magnolia uses Amazon Web Services, Inc. (AWS), Microsoft Azure (Azure) and Google Coud Platform (GCP) to provide cloud hosting services (collectively, the 'subservice organizations'). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Magnolia, to achieve Magnolia's service commitments and system requirements based on the applicable trust services criteria. The description presents Magnolia's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Magnolia's controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve Magnolia's service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of Magnolia's controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

Except for the matters described in the following paragraphs, we assert that the controls within the system were effective throughout the period February 1, 2025 to January 31, 2026 to provide reasonable assurance that Magnolia's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Magnolia's controls operated effectively throughout that period.

The accompanying description states that controls are in place to revoke logical access to systems from terminated employees. However, controls related to revoking system access from terminated employees were not operating effectively throughout the period February 1, 2025 to January 31, 2026. As a result, controls did not provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the following criteria:

- CC6.2: "Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized."
- CC6.3: "The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives."

Jan Haderka

Jan Haderka
Chief Information Security Officer
Magnolia International, Ltd.

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Magnolia International, Ltd.:

Scope

We have examined Magnolia's accompanying assertion titled "Assertion of Magnolia International, Ltd. Management" (assertion) that the controls within Magnolia's Content Management Software Services System were effective throughout the period February 1, 2025 to January 31, 2026, to provide reasonable assurance that Magnolia's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.

Magnolia uses AWS, Azure and GCP to provide cloud hosting. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Magnolia, to achieve Magnolia's service commitments and system requirements based on the applicable trust services criteria. The description presents Magnolia's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Magnolia's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Magnolia, to achieve Magnolia's service commitments and system requirements based on the applicable trust services criteria. The description presents Magnolia's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Magnolia's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Magnolia is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Magnolia's service commitments and system requirements were achieved. Magnolia has also provided the accompanying assertion (Magnolia assertion) about the effectiveness of controls within the system. When preparing its assertion, Magnolia is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our qualified opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Independence and Ethical Responsibilities

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Basis for Qualified Opinion

Magnolia states in its description that logical access to systems is revoked as part of the termination process. However, controls related to revoking system access from terminated employees were not operating effectively throughout the period February 1, 2025 to January 31, 2026. As a result, controls did not provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the following criteria:

- CC6.2: "Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized."
- CC6.3: "The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives."

Opinion

Except for the matters described in the preceding paragraphs, in our opinion, management's assertion that the controls within Magnolia's Content Management Software Services System were suitably designed and operating effectively throughout the period February 1, 2025 to January 31, 2026, to provide reasonable assurance that Magnolia's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if complementary subservice organization controls and complementary user entity controls assumed in the design of Magnolia's controls operated effectively throughout that period.

The SOC logo for Service Organizations on Magnolia's website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of Magnolia, user entities of Magnolia's Content Management Software Services during some or all of the period February 1, 2025 to January 31, 2026, business partners of Magnolia subject to risks arising from interactions with the Content Management Software Services, and those who have sufficient knowledge and understanding of the complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

A-LIGN ASSURANCE

Tampa, Florida
March 13, 2026

SECTION 3

MAGNOLIA INTERNATIONAL, LTD.'S DESCRIPTION OF ITS CONTENT MANAGEMENT SOFTWARE SERVICES SYSTEM THROUGHOUT THE PERIOD FEBRUARY 1, 2025 TO JANUARY 31, 2026

OVERVIEW OF OPERATIONS

Company Background

Magnolia was founded in 1997. The first version of the product - Magnolia content management system (CMS) - was released in 2003. Launched first as a free product under open-source software (OSS) license, Magnolia initially generated revenue from support and custom development services. In 2006, the first enterprise version was released. The first cloud version of the product was released in 2014. As of today, self-hosted and cloud versions of the product are available and serving customers as well as fully managed solution.

Magnolia is the composable Digital Experience Platform (DXP) of choice for leading enterprises in industries ranging from banking and insurance to manufacturing, media, hospitality, and retail, including Generali, Sanofi, JetBlue, Sainsbury's, BASF, ALDI, Deutsche Post and Deutsche Bahn.

Magnolia's customer base extends across verticals that require a digital presence. Approximately 30% of the customers are in Financial Services (banks and insurances), 25% in Travel and Hospitality and another 25% in News and Media with the remainder in Manufacturing, Government and Charity.

Magnolia is privately owned. The original founders sold a majority shareholding in the company to a German investment fund called Elvaston in 2017. Subsequently, in 2022 their shareholding was acquired by another German investment fund called Genui. There has been continuity in Management throughout this evolution of ownership.

Description of Services Provided

Magnolia's Content Management Software Services System is a digital experience company that provides a range of services related to digital transformation, customer experience management, and content management. The services offered by Magnolia include:

- DXP: A cloud-based platform that helps organizations create, manage, and deliver engaging digital experiences across web, mobile, and other digital channels.
- Content Management: A CMS that enables organizations to manage their digital content and deliver it across multiple channels.
- Customer Experience Management: A suite of tools and services that help organizations personalize and optimize their customers' experiences across touchpoints.
- E-commerce: A comprehensive e-commerce solution via integrations with the digital commerce platform to provide a seamless shopping experience for customers.
- Digital Transformation: Consulting and implementation services to help organizations adopt digital technologies and transform their businesses.

Overall, Magnolia aims to help organizations create and deliver outstanding digital experiences to their customers by providing features such as:

- What You See is What You Get (WYSIWYG) editing of websites
- Content pools for structured and unstructured content
- Customizable publishing and approval workflows for various types of content
- Synchronizing content among multiple websites
- Connecting multiple different systems to provide a more complete web experience
- Synchronizing and publishing marketing and other campaigns

Principal Service Commitments and System Requirements

The principal service commitments of Magnolia include:

- Quality: Magnolia is committed to providing high-quality services that meet the needs of its customers.

- Reliability: The company strives to ensure that its DXP and other services are reliable, secure, and scalable to meet the demands of its customers.
- Support: Magnolia provides ongoing support and maintenance services to ensure that its customers can fully realize the benefits of its services.
- Innovation: The company is committed to continuously improving and innovating its services to meet the evolving needs of its customers.

Individual customers' Service Level Objectives (SLOs) are subject of business negotiation and are specified in the Service Level Agreements (SLAs) attached to each customer contract.

SLOs depend on the type of contract and services provided and differ widely depending on whether the deployment is self-hosted or in the Platform as a Service (PaaS) platform.

Overall, Magnolia's service commitments and system requirements are designed to ensure that its customers can fully benefit from its services and deliver outstanding digital experiences to their customers.

Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the DXP that are designed to permit system users to access the information needed based on their role in the system while restricting them from accessing information not needed for their role.
- Use of encryption technologies to protect customer data both at rest and in transit.
- Active monitoring and alerting of runtime states.

Components of the System

Infrastructure

Primary infrastructure used to provide Magnolia's Content Management Software Services System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
AWS - K8s cluster nodes	t3a.xlarge r6a.xlarge r7a.2xlarge	Cluster nodes for the deployment of various web services
AWS - Elastic Load Balancer (ELB)	Network ELB	Used to distribute the load between the deployed containers
AWS - Volumes	GP2	Base storage for the deployed containers
VMWare	Gitlab hosting	Customer code repositories
VMWare	Identity Provider (IDP)	Apache Keycloak
AWS	N/A	Cloud hosting services
Workstations	N/A	Accessing applications and systems

Software

Primary software used to provide Magnolia's Content Management Software Services System includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
Base OS	Linux	Base operating systems on containers
Nginx	Load Balancer	Secondary load splitter between containers
Apache Tomcat	Application server	Host server for Magnolia DXP
Postgres	Database server	Storage for data
Tailscale	N/A	Virtual Private Network (VPN)
Jira and GitLab	N/A	Ticketing system
Sysdig Secure	N/A	Intrusion Detection System (IDS)/Intrusion Protection System (IPS)
AWS Shield	N/A	IDS and IPS
KeyCloak	N/A	IAM, Multifactor Authentication (MFA), and Single Sign-On (SSO)

People

Magnolia employs approximately 200 people in five main departments:

- Product Management and Development - Engineers and product managers responsible for core product development and maintenance. Also responsible for development of Software as a Service (SaaS) platform.
- Professional Services - Solution Architects, Trainers, Support personnel responsible for onboarding clients, helping them with advisory, customizations and general Magnolia-based project management. Also responsible for operation of PaaS platform.
- Marketing - Personnel responsible for website content and general promotion and communication about the product, including analyst relations and marketing campaigns.
- Sales - Responsible for product presentation and contract negotiations.
- Shared Services - Includes finance, Human Resources (HR), and Information Technology (IT) (also referred to as IT-Infrastructure or ITI team) personnel with their respective duties of managing company's financial resources, HR, and IT equipment.

Data

Data processed by the system are typically a variety of digital content types, including:

- Text: articles, blog posts, pages, and other forms of written content.
- Images: photographs, graphics, and other visual media.
- Videos: recorded footage, tutorials, and other video content.
- Audio: podcasts, music, and other audio files.
- Documents: PDFs, spreadsheets, and other office files.
- Data: customer information, sales figures, and other data sets.
- Metadata: information about the content such as title, description, keywords, author, and date of creation.

Those are the data that customers wish to make available on their website either to general public (corporate websites, ecommerce, product website, financial or other types of reports, etc.) or to limited audience (internal portals, partner portals, etc.).

The process of entering and publishing content using Magnolia CMS involves the following steps:

1. Login: The customer logs into the Magnolia CMS backend using their username and password.
2. Create or edit content: The customer creates new content or edits existing content using Magnolia's intuitive WYSIWYG editor or other custom-built editing tools.
3. Add metadata: The customer adds metadata to the content, including information such as the title, description, author, and keywords.
4. Preview: The customer previews the content to make sure it looks and behaves as expected on the website or application.
5. Publish: The customer publishes the content by clicking the "publish" button. This makes the content live and available to visitors of the website or application.
6. Approval workflows: If required, the customer may need to submit the content for approval by other users in their organization before it can be published.
7. Version control: Magnolia CMS keeps a history of all changes to the content, allowing the customer to revert to previous versions if necessary.

Overall, the process of entering and publishing content using Magnolia CMS is streamlined and user-friendly, allowing customers to focus on creating high-quality content for their audience.

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. Teams are expected to adhere to the Magnolia policies and procedures that define how services should be delivered. These are located on the Company's Intranet and can be accessed by any Magnolia team member.

Physical Security

The infrastructure supporting the production environment is hosted within AWS, Azure, and GCP. As such, the responsibility for the physical protections of this equipment is the responsibility of AWS, Azure, and GCP. For a listing of controls implemented by AWS, Azure, and GCP, please refer to the "Subservice Organizations" section, below.

Logical Access

Access to resources is restricted and requires authentication. MFA authentication is used for systems.

Data are encrypted at rest (using the industry standard Advanced Encryption Standard (AES-256) encryption algorithm, Triple Data Encryption Standard (3DES), RSA, Elliptic Curve Cryptography (ECC), and Diffie-Hellman) and in transit (Hypertext Transfer Protocol Secure (HTTPS)/ Transport Layer Security (TLS).

Customer allocated resources are separated by the virtue of using separate AWS, Azure, and GCP accounts, within each such account Virtual Private Cloud (VPC) is used to wall of resources and then for each individual cluster within VPC role-based access control (RBAC) security is used providing extra separation layer even between productive and non-productive resources and data of each customer.

Within each cluster, customers are responsible for assigning access and privileges. Magnolia employees do not have access to those resources and to the unencrypted data, unless explicitly granted by the client.

Access to the cloud-based resources and to the internal network has enforced MFA based authentication.

Principles of least privilege are used to ensure only necessary permissions are assigned and only for necessary duration of time.

Access rights are reviewed at least annually by ITI team and each review is reviewed/approved by Information Security Management System (ISMS) committee.

Both Employee access to the platform as well as Customer access to the user interface (UI) is enforced over TLS. Unique usernames are assigned to access the in-scope systems. Employee passwords conform to the complexity and other rules described in the Password Policy. Customer logins conform to the requirements specified and configured by each individual customer. Keycloak is used for IDM, MFA, and SSO. MFA is enforced.

Security training is enforced for new employees and annual refreshment training is organized by HR and overseen by Chief Information Security Officer for existing employees.

As part of the termination process HR issues offboarding checklist and coordinate with ITI team to ensure timely removal of access rights and privileges from the leavers. Similarly onboarding checklist is used to ensure access rights are granted to new hires in timely manner and upon receiving the necessary trainings.

When hiring new employees the checks and the process itself is done according to the description in the Hiring Policy.

Computer Operations - Backups

Laptop backups are done every 12 hours to the encrypted drives on the cloud. Cloud based server systems have nightly backups configured in the cloud-based storage. The backups are realized as PIT (Point In-time) recovery hence allowing them to go back to the data at any point in time as long as history of the data is preserved - annual for critical platform and internal systems, contract-specific time period for customer data.

The accuracy of customer data, availability of backups, and backup restore capability are the responsibility of the clients. Refer to the “Complementary User Entity Controls” section below.

Computer Operations - Availability

Availability of the platform is subject to many specific variables and subsystems such as data center facility, disk storage, computing, and network resources. Since the goal of the platform is to serve data to customer’s clients, generally high availability is demanded. The default provided value is 99.5% (baseline as per AWS, Azure, and GCP default availability). This availability can be increased by scaling customer deployment to multiple geo-separated clusters as well as by adding extra redundancy layers and extra security measures. Those are subject to the needs of customer specified within contract.

Platform provides automated monitoring for critical resources, namely the computing power, memory usage, disk usage, network input/output (IO) on the level of individual resources, whole clusters as well as health of the platform deployments. Metrics from the measurement are available to each customer within their cockpit for overview and escalation. Furthermore, internal alerts are delivered to the operation team as well as to the helpdesk should any of the values for any of the monitored metric fall out of the usual range. This includes raising the alert when trigger value is reached as well as canceling the alert when normal operational value of affected system is reached again. Notifications are delivered to internal communication tool (slack channels), over email as well as automated calls.

As for patching the systems, customers are notified about new releases and those are made available to them (and automatically deployed in case of SaaS), however in case of PaaS customers themselves are responsible applying those patches by triggering the build and deployment on their own clusters.

Change Control

Magnolia's secure development policy mandates and implemented processed enforce that code changes have to be recorded in version control system (VCS) system and code is tested prior to the deployment. Deployments of code are fully automated and automatically rejected if tests failures occur.

Code changes are tracked via ticketing system (either Jira or Gitlab).

In general, code changes are initiated by creating the ticket describing desired change. After qualifying and developing the ticket to contain necessary details, code changes are implemented, reviewed by other independent team members prior to being merged into the full code base.

Code changes including security patches are going through the same process.

Data Communications

Web Application Firewall (WAF) is deployed for each customer shielding the deployment. Similarly separate instance of WAF is used to protect central platform resources.

The deployment of resources is distributed between different availability zones at minimum or at customer request possibly along multiple data centers. Each of the resources within the deployment is replicated providing redundancy within the system itself and ensuring there is no single point of failure in any part of the platform. The correctness of the setup as well as working of the elements is ensured via annual disaster recovery (DR) test confirming various scenarios of partial or complete disaster.

To ensure maximum security, annual system-wide penetration test is performed by an independent third-party (Compass Security).

Vulnerability scanning is performed weekly, and any reported findings are reviewed and fixed. Furthermore, Magnolia actively scans for vulnerabilities in deployed containers using cloud-based tools.

Magnolia also actively scans for intrusions using an ID/IPS tool.

Boundaries of the System

The scope of this report includes the Content Management Software Services System performed in the Münchenstein, Switzerland facilities.

This report does not include the cloud hosting services provided by AWS, Azure, and GCP at multiple facilities.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user in the 12 months preceding the end of the review period.

Incidents in the Last 12 Months

2026-01-23 incident (Swiss hosting outage):

Start time: 10:56 UTC

Resolved to normal operation: 12:18 (UTC)

Impacted services:

- DX Cloud customer cockpit (EU)

- Default IDP (EU)
- DNS
- K8s admin interface - both UI and API (EU)
- CI/CD services (EU)
- Metric collection and storage (EU)

Central log storage (EU)

Root cause: Inter-datacenter Layer 2 network connections between two Swiss hosting datacenters hosting DX Cloud platform services were interrupted causing connection failures to the DX Cloud services above.

Remediation:
- For the duration of the incident, all traffic was explicitly routed to the primary DC/AZ to avoid use of unreliable L2 connection.

Notification: Customer website availability hosted on other data centers (AWS, Azure) were not affected.

Please note this did not reach our defined level of a critical incident based on the remediation performed and the minimal impact to our services.

Criteria Not Applicable to the System

All Common Criteria/Security criteria were applicable to the Magnolia's Content Management Software Services System.

Subservice Organizations

Cloud providers (AWS, Azure, GCP) directly support the in-scope systems through its cloud hosting services. Cloud providers house in-scope networking, database, and application assets required for Magnolia to perform the in-scope services.

Subservice Description of Services

Hosting and operation of alerting, monitoring and remediation services for the infrastructure operating and maintenance of the platform deployments for the clients:
- Kubernetes Management Environment Rancher
- Management Cockpit
- Logging and monitoring services Loki, Grafana and Thanos

Complementary Subservice Organization Controls

Magnolia's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to Magnolia's services to be solely achieved by Magnolia control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Magnolia.

The following subservice organization controls should be implemented by AWS, Azure, and GCP and included in this report to provide additional assurance that the trust services criteria are met:

Subservice Organization - AWS		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4, CC7.2	Physical access to data centers is approved by an authorized individual.

Subservice Organization - AWS		
Category	**Criteria**	**Control**
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.

Subservice Organization - Azure		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4, CC7.2	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Electronic IDSs are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		The badge access system logs successful and failed physical access attempts and the logs could be pulled for review when necessary.

Subservice Organization - GCP		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4, CC7.2	Data center server floors network rooms and security systems are physically isolated from public spaces and/or delivery areas.
		Access to sensitive data center zones requires approval form authorized personnel and is controlled via badge access readers, biometric identification mechanism, and/or physical locks.
		Data center perimeters are defined and secured via physical barriers.
		Access lists to high security areas in data centers are reviewed on a periodic basis and inappropriate access is removed in a timely manner.
		Visitors to data center facilities must gain approval from authorized personnel, have their identity verified at the perimeter, and remain with an escort for the duration of the visit.

Subservice Organization - GCP		
Category	**Criteria**	**Control**
		Security measures utilized in data centers are assessed annually and the results are reviewed by executive management.
		Data centers are continuously staffed and monitored by security personnel using real time video surveillance and/or alerts generated by security systems.

Magnolia management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as SLAs. In addition, Magnolia performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing and reconciling output reports
- Holding periodic discussions with vendors and the subservice organizations
- Reviewing attestation reports over services provided by vendors and the subservice organizations
- Monitoring external communications, such as customer complaints relevant to the services provided by the subservice organizations

COMPLEMENTARY USER ENTITY CONTROLS

Magnolia's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria related to Magnolia's services to be solely achieved by Magnolia's control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Magnolia's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to Magnolia.
2. User entities are responsible for notifying Magnolia of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Magnolia services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Magnolia services.
6. User entities are responsible for providing Magnolia with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Magnolia of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.