



mxHero, Inc.

Report on mxHero's Description of its Mail2Cloud System and on the
Suitability of the Design and Operating Effectiveness of Controls Relevant to Security
Throughout the Period July 16, 2024 to July 15, 2025 (Type 2)

SOC 2 ® - SOC for Service Organizations: Trust Services Criteria





TABLE OF CONTENTS

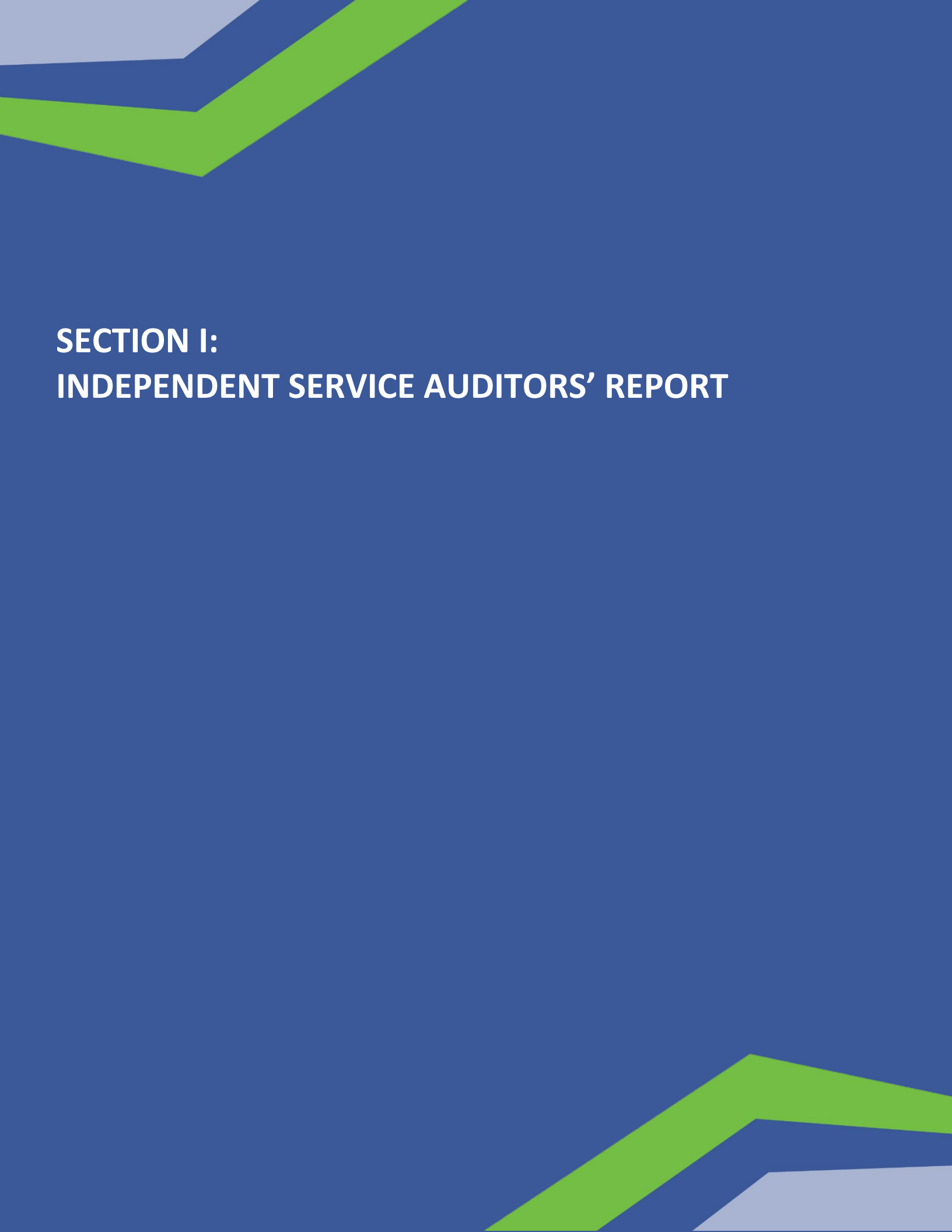
I. INDEPENDENT SERVICE AUDITORS’ REPORT.....3

II. ASSERTION OF THE MANAGEMENT OF MXHERO, INC. 7

III. MXHERO’S DESCRIPTION OF ITS MAIL2CLOUD SYSTEM.....10

IV. APPLICABLE TRUST SERVICES CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS 27

V. OTHER INFORMATION PROVIDED BY MXHERO, INC. 60

The page features a solid blue background. In the top-left corner, there are overlapping geometric shapes in light blue and green. In the bottom-right corner, there are similar overlapping shapes in green and light blue.

SECTION I: INDEPENDENT SERVICE AUDITORS' REPORT

INDEPENDENT SERVICE AUDITORS' REPORT

To: **mxHero, Inc.**

San Francisco, California

Scope

We have examined mxHero, Inc.'s ("mxHero") accompanying description of its system titled "mxHero's Description of its Mail2Cloud System throughout the period July 16, 2024 to July 15, 2025" ("description") based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance – 2022)* in AICPA, *Description Criteria* ("description criteria"), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period July 16, 2024 to July 15, 2025, to provide reasonable assurance that mxHero's service commitments and system requirements were achieved based on 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 (With Revised Points of Focus – 2022)* in AICPA, *Trust Services Criteria*.

mxHero uses a subservice organization for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at mxHero, to achieve mxHero's service commitments and system requirements based on the applicable Trust Services Criteria. The description presents mxHero's controls, the applicable Trust Services Criteria, and the types of complementary subservice organization controls assumed in the design of mxHero's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, 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 mxHero, to achieve mxHero's service commitments and system requirements based on the applicable Trust Services Criteria. The description presents mxHero's controls, the applicable Trust Services Criteria, and the complementary user entity controls assumed in the design of mxHero'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.

The information included in Section V, "Other Information Provided by mxHero, Inc." is presented by mxHero management to provide additional information and is not a part of mxHero's description. This information has not been subjected to the procedures applied in the examination of the description, the suitability of the design and the operating effectiveness of the controls to achieve mxHero's service commitments and system requirements based on the applicable Trust Services Criteria, and accordingly, we express no opinion on it.

Service Organization's Responsibilities

mxHero 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 mxHero's service commitments and system requirements were achieved. mxHero has provided an assertion titled "Assertion of the Management of mxHero, Inc." ("assertion") about the description and the suitability of design and operating effectiveness of the controls stated therein. mxHero is responsible for preparing the description and assertion; including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable Trust Services Criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants.

Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable Trust Services Criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our qualified opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls includes the following:

- 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 the description is presented in accordance with the description criteria.
- 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.
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable Trust Services Criteria.
- Evaluating the overall presentation of the description.

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

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the System that individual users may consider important to meet their informational needs.

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.

Description of Tests of Controls

The specific controls tested and the nature, timing, and results of those tests are presented in Section IV of our report titled "Applicable Trust Services Criteria, Related Controls, and Tests of Controls."

Basis for Qualified Opinion

mxHero's Access Control Policy states that the Company performs access reviews at least quarterly. However, as noted in Section IV, controls related to the Company's access reviews were not consistently performed during the period July 16, 2024 to July 15, 2025. As a result, during the period July 16, 2024 to July 15, 2025, the controls were not operating effectively to provide reasonable assurance that mxHero's service commitments and system requirements were achieved based on the applicable Trust Services 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.

Qualified Opinion

In our opinion, except for the matter referred to in the "Basis for Qualified Opinion" paragraph, in all material respects:

1. The description presents mxHero's Mail2Cloud System that was designed and implemented throughout the period July 16, 2024 to July 15, 2025 in accordance with the description criteria.
2. The controls stated in the description were suitably designed throughout the period July 16, 2024 to July 15, 2025, to provide reasonable assurance that mxHero's service commitments and system requirements would be achieved based on the applicable Trust Services Criteria, if its controls operated effectively throughout the period and if the subservice organization and user entities applied the complementary controls assumed in the design of mxHero's controls throughout the period.
3. The controls stated in the description operated effectively throughout the period July 16, 2024 to July 15, 2025, to provide reasonable assurance that mxHero'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 mxHero's controls operated effectively throughout the period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV of our report titled "Applicable Trust Services Criteria, Related Controls, and Tests of Controls" is intended solely for the information and use of mxHero; user entities of mxHero's system during some or all of the period July 16, 2024 to July 15, 2025, business partners of mxHero's subject to risks arising from interactions with mxHero's system; practitioners providing services to such user entities and business partners; prospective user entities and business partners; and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable Trust Services Criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

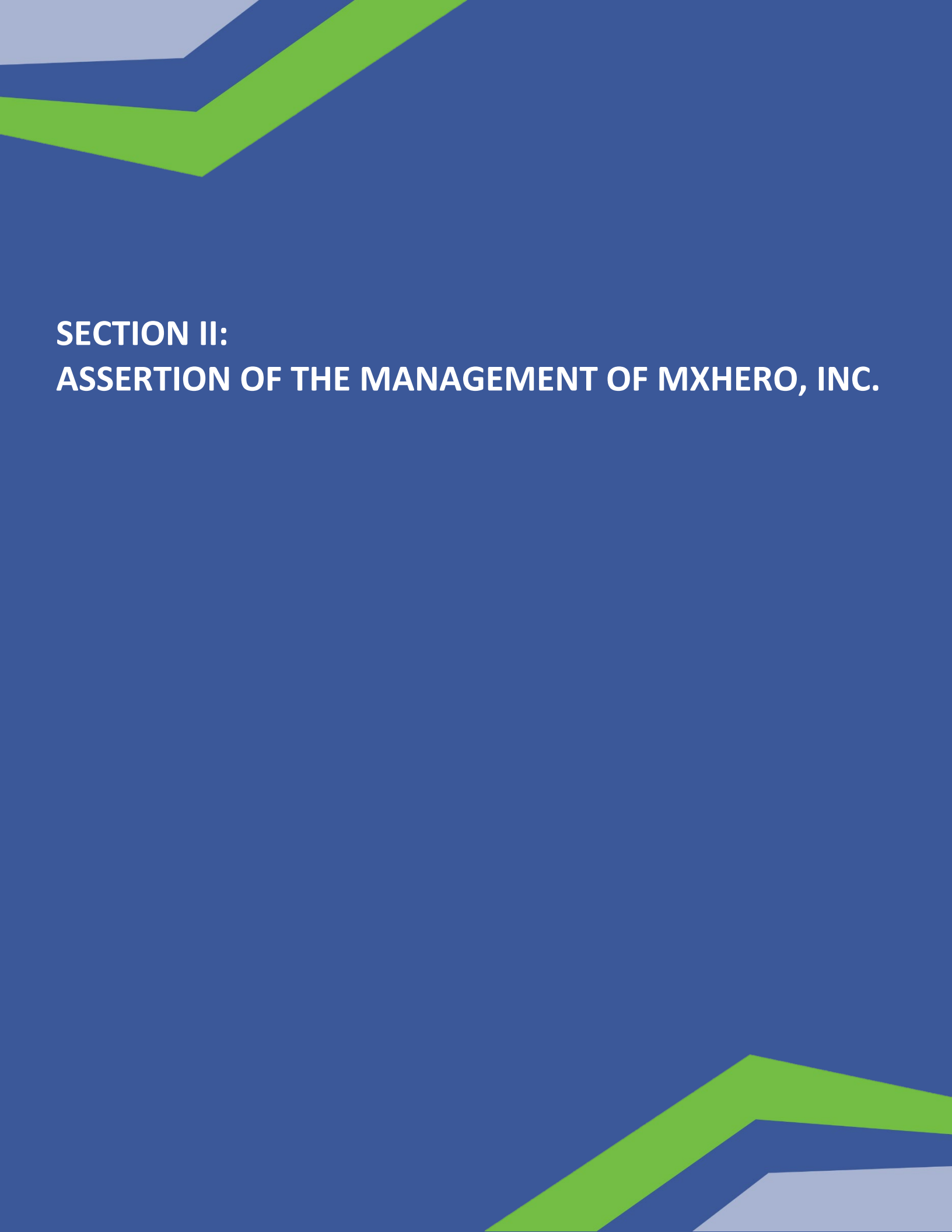
This report is not intended to be and should not be used by anyone other than these specified parties.

Dan D'Arata Senior

DANSA D'ARATA SOUCIA LLP

Buffalo, New York

March 6, 2026

The page features a solid blue background. In the top-left corner, there are overlapping geometric shapes in light blue and green. In the bottom-right corner, there are similar overlapping geometric shapes in green and light blue.

SECTION II: ASSERTION OF THE MANAGEMENT OF MXHERO, INC.



Assertion of the Management of mxHero, Inc.

We have prepared the accompanying description of our system titled “mxHero’s Description of its Mail2Cloud System throughout the period July 16, 2024 to July 15, 2025” (“description”) based on the criteria for a description of a service organization’s system identified in DC section 200, *2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2® Report (With Revised Implementation Guidance – 2022)* in AICPA, *Description Criteria* (“description criteria”). The description is intended to provide users with information about the System, particularly system controls intended to meet 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 (With Revised Points of Focus – 2022)* in AICPA, *Trust Services Criteria*, throughout the period July 16, 2024 to July 15, 2025.

mxHero uses a subservice organization for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed are necessary, along with controls at mxHero, to achieve mxHero’s service commitments and system requirements based on the applicable Trust Services Criteria. The description presents mxHero’s controls, the applicable Trust Services Criteria, and the types of complementary subservice organization controls assumed in the design of mxHero’s controls. The description does not disclose the actual controls at each subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at mxHero, to achieve mxHero’s service commitments and system requirements based on the applicable Trust Services Criteria. The description presents mxHero’s controls, the applicable Trust Services Criteria, and the complementary user entity controls assumed in the design of mxHero’s controls.

We confirm, to the best of our knowledge and belief, that:

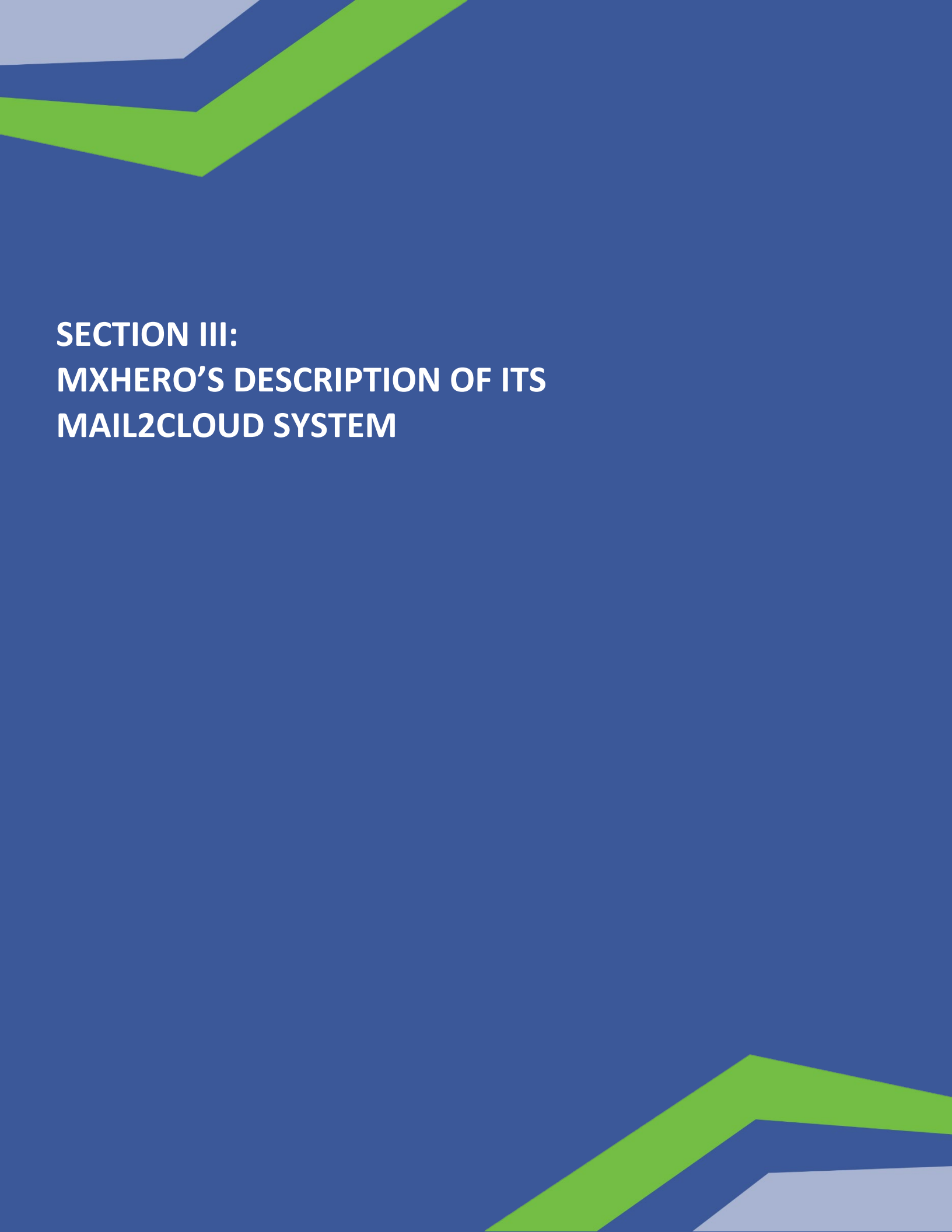
- 1) The description fairly presents the System throughout the period July 16, 2024 to July 15, 2025, based on the following description criteria:
 - a. The description contains the following information:
 - i. The types of services provided.
 - ii. The components of the System used to provide the services, which are as follows:
 1. Infrastructure - IT and other hardware (for example, computers, equipment, mobile devices, and telecommunication networks).
 2. Software - The application programs and IT system software that supports application programs (operating systems, middleware, and utilities).
 3. People - The personnel involved in the governance, operation and use of the System (developers, operators, entity users, vendors and managers).
 4. Procedures - The automated and manual procedures.
 5. Data - Transaction streams, files, databases, tables and output used or processed by the System.
 - iii. The boundaries or aspects of the System covered by the description.
 - iv. For information provided to, or received from, subservice organizations and other parties:
 1. How the information is provided or received and the role of the subservice organizations and other parties.
 2. The procedures the service organization performs to determine that such information and its processing, maintenance and storage are subject to appropriate controls.
 - v. The applicable Trust Services Criteria and the related controls designed to meet those criteria, including, as applicable, the following:
 1. Complementary user entity controls contemplated in the design of the service organization’s system.

- vi. The service organization presents the subservice organization using the carve-out method. The description includes:
 - 1. The nature of the services provided by the subservice organization.
 - 2. Each of the applicable Trust Services Criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria.
 - vii. Any applicable Trust Services Criteria that are not addressed by a control and the reasons.
 - viii. Relevant details of changes to the service organization's system during the period covered by the description.
 - b. The description does not omit or distort information relevant to the service organization's system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the System that each individual user may consider important to his or her own particular needs.
- 2) The controls stated in the description were suitably designed to meet the applicable Trust Services Criteria throughout the period July 16, 2024 to July 15, 2025.
- 3) The controls stated in the description operated effectively throughout the period July 16, 2024 to July 15, 2025, to meet the applicable Trust Services Criteria.

We state in our Access Control Policy that the Company performs access reviews at least quarterly. However, as noted in Section IV, controls related to the Company's access reviews were not consistently performed during the period July 16, 2024 to July 15, 2025. As a result, during the period July 16, 2024 to July 15, 2025, the controls were not operating effectively to provide reasonable assurance that mxHero's service commitments and system requirements were achieved based on the applicable Trust Services 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.

mxHero, Inc.

The page features a solid blue background. In the top-left corner, there are overlapping geometric shapes in light blue and green. In the bottom-right corner, there are similar overlapping geometric shapes in green and light blue.

SECTION III: MXHERO'S DESCRIPTION OF ITS MAIL2CLOUD SYSTEM

Company Overview and Background

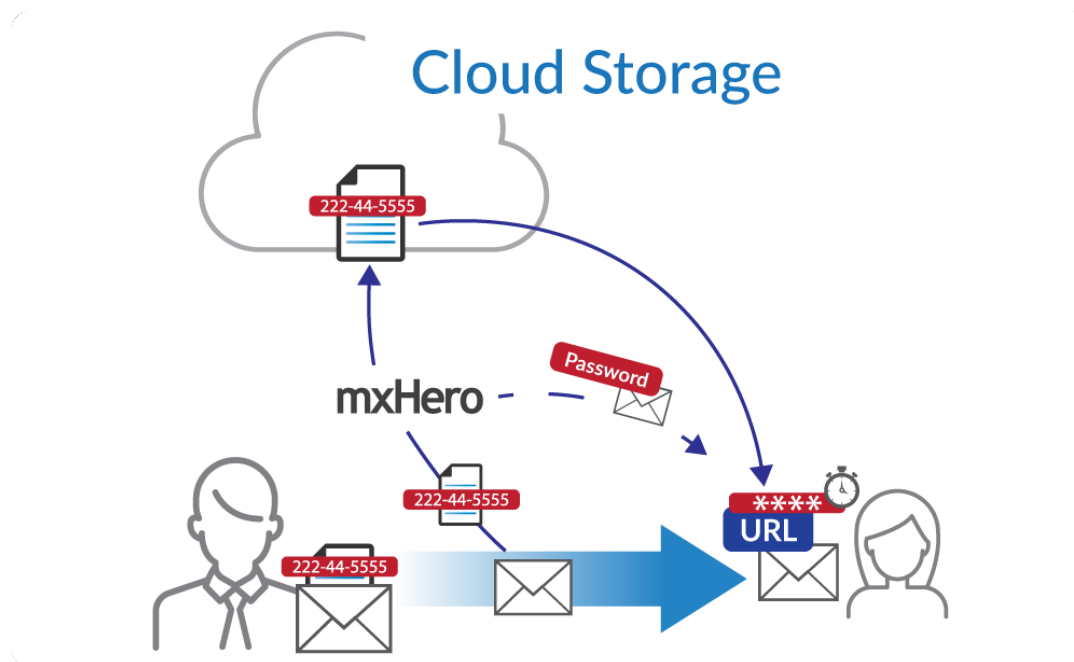
mxHero, Inc. ("mxHero" or "the Company") provides integration between email systems and public cloud storage services to customers globally. The Company was founded in 2011 to provide email enhancement services to businesses of all sizes.

Overview of Products and Services

mxHero's core application, Mail2Cloud ("the System"), is a multi-tenant cloud service that serves as a digital bridge between email systems, whether cloud (e.g., Google Workspace, Microsoft 365) or on premises (e.g., Microsoft Exchange), and business class cloud storage services (e.g., Box, Dropbox, Egnyte, Microsoft OneDrive, SharePoint Online, Google Drive). The integration of email with enterprise cloud storage provides many benefits to mxHero's customers, such as:

- **Email security** - Protect email content by moving, for example, file attachments out of insecure email and into secure cloud storage prior to delivery.
- **Email governance** - Capture email (message and body) and store it in the client's sanctioned cloud storage service for governance controls, such as, legal holds and retention policies.
- **Cost reduction** - Reduce infrastructure costs by moving copious and duplicative email content out of expensive on-premises email systems into near unlimited cloud storage services.
- **Email management** - Automatically capture, classify, and file email correspondence into targeted cloud storage folders.
- **Ease of use** - All the above benefits are delivered automatically, not requiring installation of software or training on the part of the end-user.

Deployment of mxHero typically takes less than 90 minutes, regardless of the size of the organization. Depending on which use-case the customer is pursuing, mxHero processes email messages in-flight (being sent and received) or are at-rest (in user inboxes, email servers or archives).



Example mxHero security use-case



Principal Service Commitments and System Requirements

mxHero services most of its clients through its Amazon Web Services (AWS) service cluster; the scope of this report is limited to clients serviced through AWS. This cluster is managed by a select team of highly qualified personnel with decades of enterprise and telco operational experience.

mxHero’s service is topologically equivalent to a network router. mxHero is not designed to retain data. The service acts as a gateway where email is temporarily processed for integration with cloud storage systems. Like a router, mxHero’s services possess very little internal storage, only enough to process email in transit. Once processed, mxHero deletes local temporary copies to allow the System to continue processing inbound messages. mxHero’s systems are not designed to hold messages for longer than needed for the express purpose of processing. Processing normally takes less than 30 seconds to occur. As an additional precaution, all temporary storage used for processing utilizes encrypted file systems ensuring that data is always encrypted at rest.

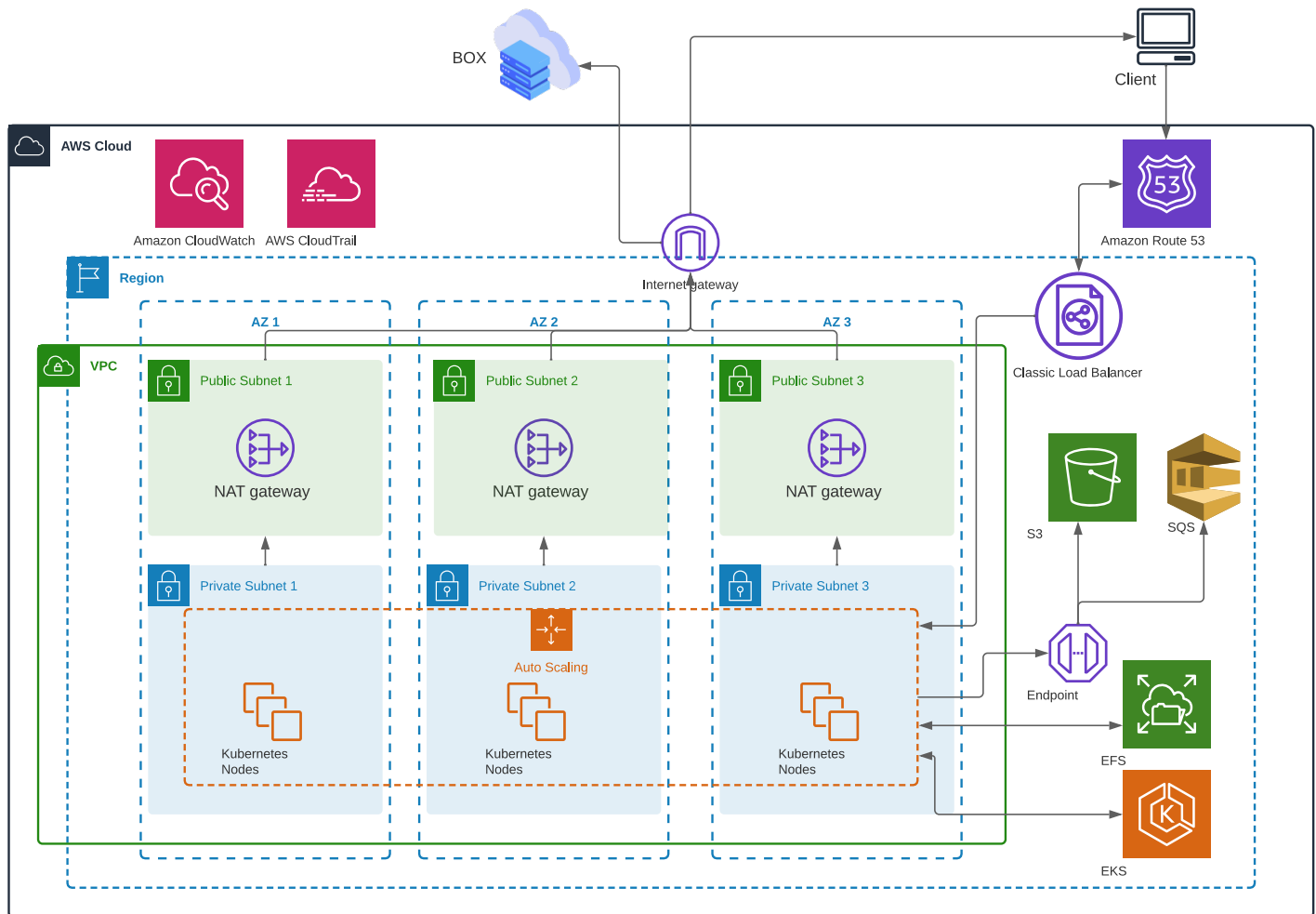
mxHero establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in mxHero’s system policies and procedures, system design documentation, and contracts with customers. Information security policies define the Company’s approach to how systems and data are protected. These include policies around how the service is designed and developed, how the System is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the System.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

Trust Services Criteria	Service Commitments	System Requirements
Security	- mxHero will employ administrative and technical measures in accordance with applicable industry practices to protect the System and prevent the accidental loss or unauthorized access, use, alteration, or disclosure of customer data under its control during each order term. - All data transmitted between the Company and the users of the System is protected using transport layer security (TLS) and HTTP strict transport security (HSTS). - Access to environments that contain customer data requires a series of authentication and authorization controls, including multi-factor authentication (MFA). - The Company monitors critical infrastructure for security-related events by using a custom implementation of open source and commercial technologies.	- Employee provisioning and deprovisioning standards - Logical access controls such as user IDs and passwords to access the System - Encryption of data in transit over public networks - Security monitoring controls

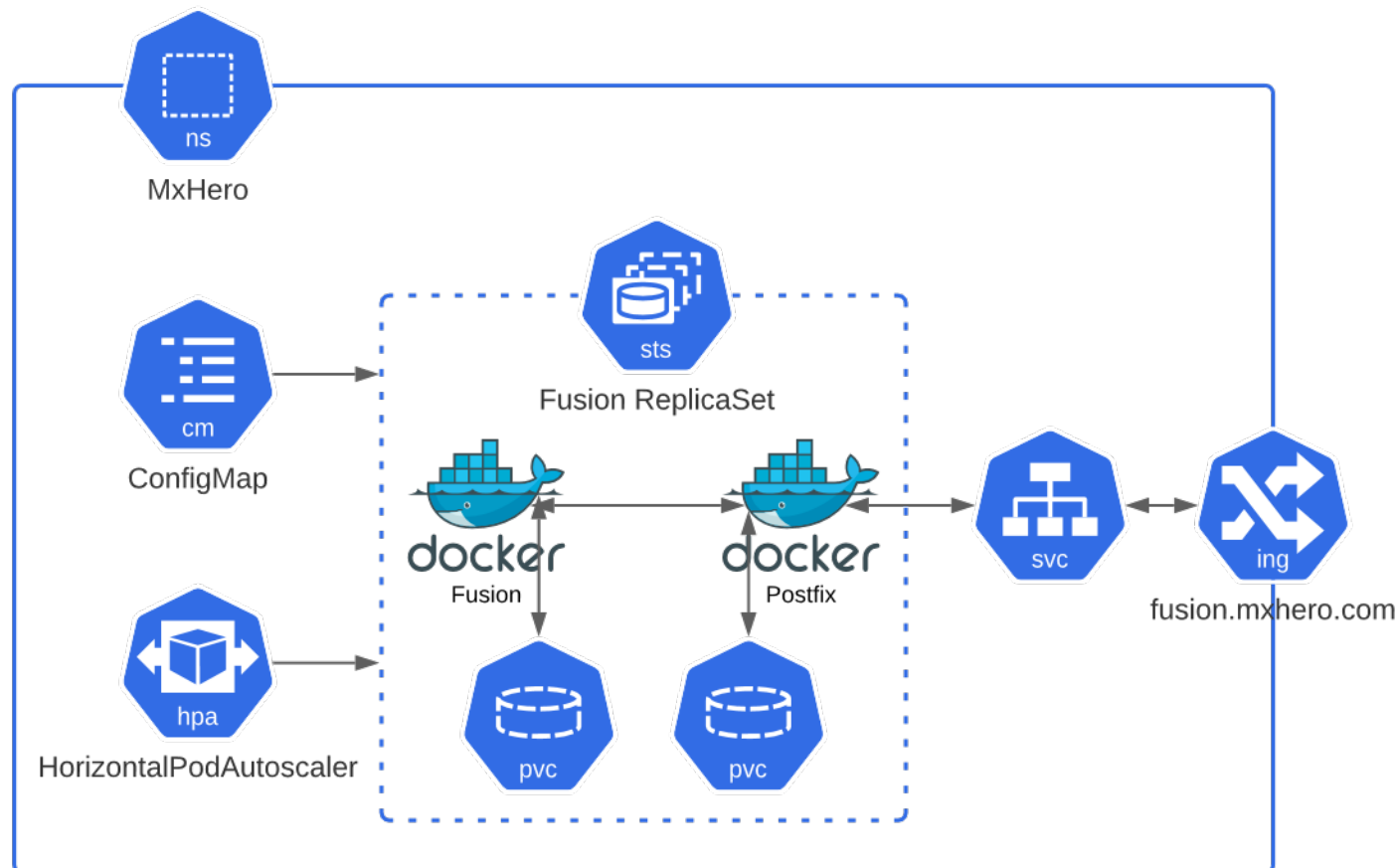
Components of the System

Infrastructure



mxHero's AWS cluster architecture has been delivering high reliability and security to millions of users for more than a decade. Deployed in the United States at AWS east-1, the cluster operates in a private network gated to the Internet through highly restricted firewalls. All internal systems are continuously monitored for security and availability. Access to the System is limited to a small group of highly qualified administrators authenticated by MFA in two stages, once for access to the network and again to access any of the subsystems.

mxHero employs modern container technology to ensure maximum availability of its service. The service delivers high availability through continual and automated monitoring and failover, controlled service releases over stage and production environments across multiple availability zones. Front-facing load balancers provide additional protection against potential denial-of-service attacks. Docker and Kubernetes container technology enables auto-scaling to continuously adjust to growing demand without downtime while simplifying new deployments and upgrades. Scheduled bi-weekly service updates fully refresh virtual machines with clean installs.



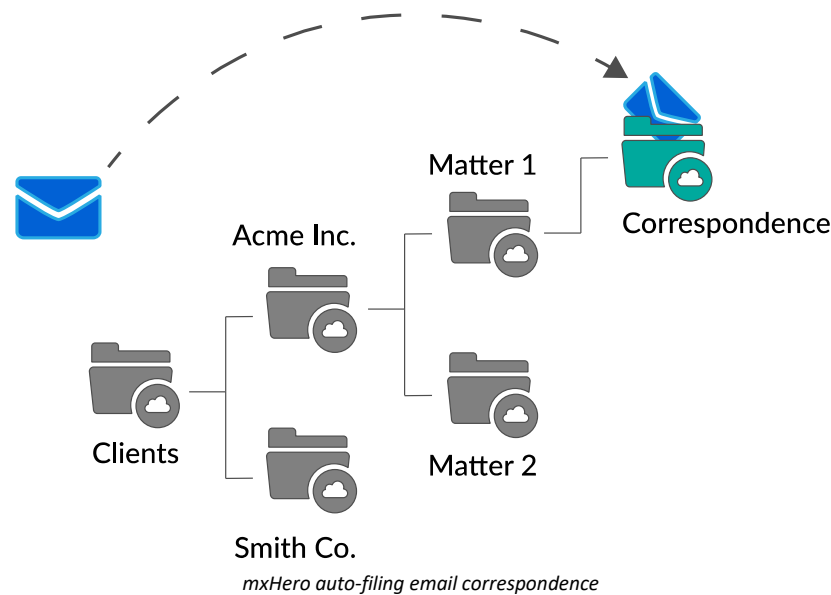
Software

The System is a Linux cluster application developed and maintained by mxHero's in-house software engineering group. The software engineering group enhances and maintains the System to provide service for the Company's customers. mxHero's software is not sold on the open market.

The System captures email either passively through message routing changes (e.g., the customer routes email through mxHero) or actively through secure IMAP access to email stores. After the capture phase, mxHero processes the message (and attachments) following a set of rules configured by the customer. These rules leverage mxHero's ability to examine all aspects of the email, including message headers, body, and attachment content. The System can look for key words, patterns and cross reference results with customer provided databases. Based on the processing phase, mxHero can set prescriptive filing or security rules on content.

If mxHero is configured to strip out email attachments and replace them with secure cloud storage links, customer defined rules determine what storage account and which folder the removed email attachments are stored. Furthermore, the security setting of the link placed in the email is determined. For example, a company can determine that all email attachments with social security numbers in them will be delivered through cloud storage links that require a password from the recipient.

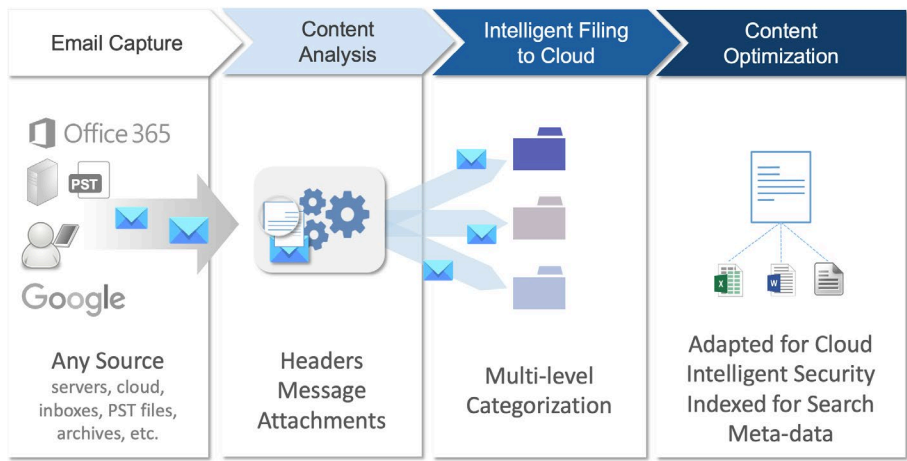
SECTION III - MXHERO’S DESCRIPTION OF ITS MAIL2CLOUD SYSTEM
THROUGHOUT THE PERIOD JULY 16, 2024 TO JULY 15, 2025



In the case where mxHero is used as an email management tool, entire email messages and their attachments can be filed into the Company’s cloud storage service. Based on provided rules, mxHero can save email messages following specific customer provided taxonomies, for example, for a legal firm this could be in folders specific for each legal matter. For a construction company, this could be folders organizing email correspondence by construction project.

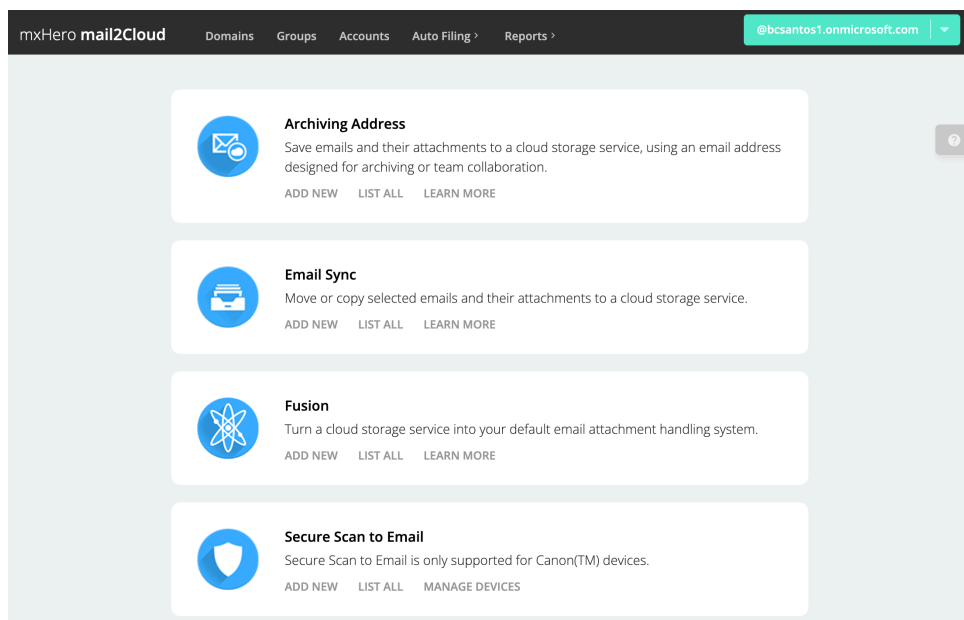
All content uploaded by mxHero is optimized for cloud storage usage. Messages are parsed for key identifiers like sender, recipient, date etc. These identifiers are set as metadata tags or folder hierarchies.

How mxHero Works



Customer administration of mxHero is done through a web-based administrative console. From the console, the client can set filing and security rules as well as define one or more cloud storage targets. The panel also provides diagnostic tools.

SECTION III - MXHERO'S DESCRIPTION OF ITS MAIL2CLOUD SYSTEM
THROUGHOUT THE PERIOD JULY 16, 2024 TO JULY 15, 2025



mxHero administrative dashboard (web)

Third-Party Apps Used

mxHero relies on the following third-party apps to deliver our services:

- **AWS** - Cloud computing web services platform used for infrastructure and data storage
- **Google Workspace** - Platform for productivity and collaboration tools including email, document storage, and enterprise identity management (e.g., SSO)
- **Salesforce** - CRM system storing customer and licensing information
- **Zendesk** - Support system used to interact with customers
- **Bitbucket** - Source code management system, provided by Atlassian
- **Jira** - Task and ticket tracking system, provided by Atlassian
- **Vanta** - SOC 2® compliance monitoring system
- **Detectify** - Vulnerability scanner system enabling automated scheduled security scans
- **Zoom** - Conferencing system utilized to communicate with customers
- **Box** - Cloud content management system

People

mxHero is organized into the following functional areas:

Corporate - Executives, senior operations staff, and the Company's administrative support staff, such as legal, compliance, internal audit, training, contracting, accounting, finance, and human resources. These individuals use the System primarily as a tool to measure performance at an overall corporate level. This includes reporting done for internal metrics as well as for mxHero's user entities.

SECTION III - MXHERO'S DESCRIPTION OF ITS MAIL2CLOUD SYSTEM THROUGHOUT THE PERIOD JULY 16, 2024 TO JULY 15, 2025

Development/Operations - Staff that administers the development and provision of mxHero's cloud services. They develop the software following the product roadmap, fix issues identified in the current system, monitor the health of the production systems, adhere and maintain security best practices and provide quality assurance (QA) reviews prior to the release of any new code. This group also interacts with stakeholders, whether they be internal stakeholders, such as the sales teams providing customer feedback or delivery teams needing guidance or adjustments as needed for customer onboarding, or external stakeholders through customer support tickets.

Data

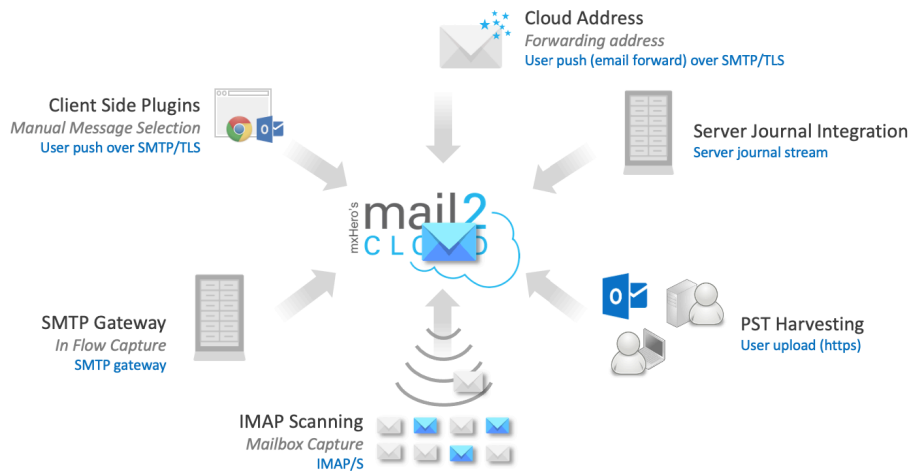
Data, as defined by mxHero, constitutes the following:

- Email messages
- Output reports
- Input reports
- System files
- Error logs

Email data enters mxHero's systems through a variety of pathways. Customers configure their email systems to either route email traffic through mxHero or allow mxHero to access email content directly from email stores (e.g., secure IMAP).

mxHero Message Capture Options

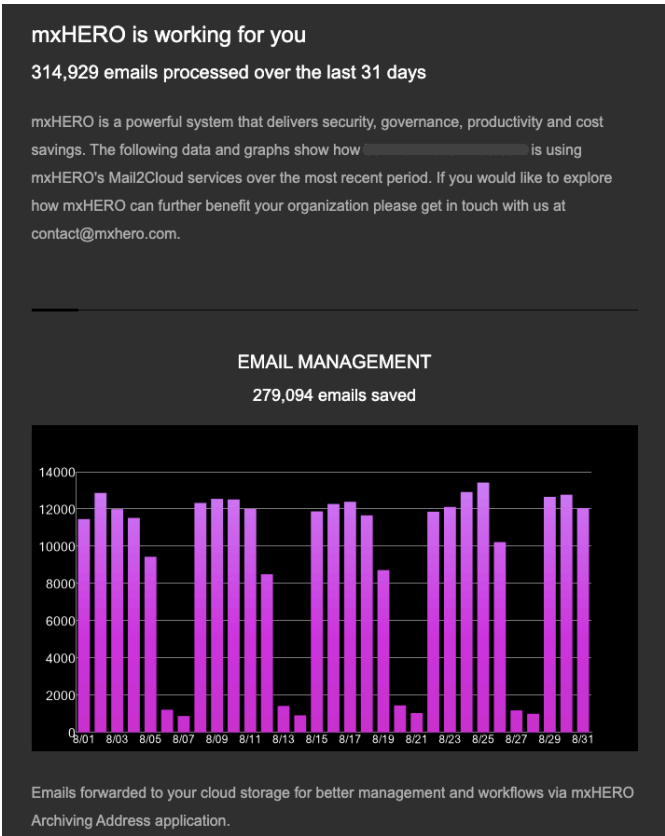
method of data transmission



mxHero email ingestion options

mxHero maintains records of messages processed. These records constitute basic message metadata like sender, recipient, date and which mxHero rules were applied. These records are provided for the benefit of the customer and are accessible via the customer's mxHero dashboard.

Service usage statistics are generated monthly and sent to customers. These reports detail daily usage of the mxHero services employed by the customer.



mxHero customer usage report

Processes and Procedures

mxHero does not retain customer emails. Messages are transient, held only during processing. Processing typically results in either parts of the message, like the attachments, being removed from the email and uploaded into the customer’s cloud storage service or allowed to flow through untouched. How processing occurs is dependent on the rules set by the customer in mxHero’s dashboard. For processing, mxHero saves the email to temporary and encrypted storage. Processing an email typically takes around 10 seconds.

mxHero maintains two distinct environments for its services, one for staging and the other for production. Furthermore, production environments are in multiple AWS availability zones. The stage environment is where the Development team and select stakeholders can test new or fixed code prior to release to the production environment. Access to these environments are controlled via a centralized and secured directory (private keys and MFA). Only a select group of employees have access to either environment. All access to the stage or production environments is done through encrypted channels and require MFA.

mxHero software development follows an agile methodology and operates on a two-week sprint cadence. At the end of every sprint, the System in stage is subjected to a battery of automated and manual tests by dedicated QA staff. Furthermore, coinciding with the two-week release cadence, a battery of automated security tests are performed with reports sent to key internal staff.

Security Management

mxHero is a collective responsibility from the top to bottom of the Company. The CTO and COO continuously implement security actions through their teams and meet weekly to discuss security efforts with the CEO. They are responsible for developing, maintaining, and enforcing mxHero's information security policies. The information security policies are reviewed annually by the CTO, COO and CEO, and are approved by management.

As the Information Security team maintains security, it monitors known incidents and patches as well as results from recent vulnerability assessments and addresses necessary changes to the policies and procedures. Such changes can include a reclassification of data, a reassessment of risk, changes in incident response plans, and a verification of responsibilities for authorizing and monitoring accesses. Changes are reviewed and communicated during weekly IT maintenance meetings or through system alerts.

During annual security training and awareness programs, management ensures communication of the latest security policies as well as written job descriptions for security management.

Additionally, management is responsible for ensuring business associate agreements are current for third parties and for updating the annual IT risk assessment.

Change Management

mxHero has a formalized change management process in place, which requires identification and recording of significant changes, assessment of risk and potential effect of such changes, approval of proposed changes, and testing of changes to verify operational functionality. Proposed changes are evaluated to determine if they present a security risk and what mitigating actions, including employee and user entity notifications, must be performed. The Information Security team meets weekly to review and schedule changes to the IT environment.

Emergency changes follow the formalized change management process, but at an accelerated timeline. Prior to initiating an emergency change, necessary approvals are obtained and documented.

Changes to infrastructure and software are developed and tested in a separate development or test environment before implementation. Additionally, developers do not have the ability to migrate changes into production environments.

mxHero has a formalized security and systems development methodology that includes project planning, design, testing, implementation, maintenance, and disposal or decommissioning.

mxHero uses a standardized server build (predefined Docker images) to help secure its servers, and it conducts biweekly vulnerability assessments to identify potential system vulnerabilities. Patches are applied regularly in accordance with mxHero's patch management process.

System Monitoring

The Information Security team uses a variety of security utilities to identify and detect possible security threats and incidents. These utilities include, but are not limited to, firewall notifications, intrusion detection system (IDS) alerts, vulnerability assessment reports, and operating system event logs. These alerts and notifications are reviewed daily by the Information Security team using a security incident and event monitoring flowing through AWS Athena, JumpCloud, OSSEC and email notifications.

Incident Management

Security incidents and other IT-related problems are reported to the help desk. Issues are tracked using a help desk ticket and monitored until resolved.

Data Backup and Recovery

mxHero uses data replication and AWS backups for data files and software. Access to backup devices, scheduling utilities, systems, and media is restricted to authorized personnel.

System Account Management

mxHero has implemented role-based security to limit and control access within the System. Employees are granted logical and physical access to in-scope systems based on documented approvals by appropriate management personnel. mxHero's customers (user entities) are approved for access by an authorized user. The ability to create or modify user access accounts and user access privileges is limited to authorized personnel. User access is reviewed quarterly to verify whether individuals' access is necessary for their job functions and to identify the existence of inappropriate accounts.

Upon employee termination, management provides IT personnel with an employee termination request. IT reconciles the termination report with current access privileges to determine if access has been appropriately removed or disabled. Dormant network accounts are disabled after 90 days of inactivity, and dormant Mail2Cloud accounts are disabled after 45 days of inactivity.

Administrative access to Active Directory, Unix, and Mail2Cloud servers and databases is restricted to authorized employees.

Unique user identification numbers, names, and passwords are required to authenticate all users to the System, as well as to member services, and client reporting websites. Password parameters consist of the following:

- Passwords contain a minimum of eight characters, including one non-alphanumeric, upper-case, lower-case, and special character.
- Passwords expire every 90 days.
- Log-on sessions are terminated after six failed log-on attempts prior to logout.
- Users cannot reuse the last three passwords.

Vendor Management

To initiate a vendor relationship, management negotiates and manages the vendor contract clauses and additional data protection agreements with vendors who process or store the Company's data, customer data, or employee data, as well as systems that connect to the Company's systems. Management also manages the vendor security risk assessment process. The Company maintains operational processes to assess security risk considerations related to vendors. These vendors are required to undergo an initial security risk assessment prior to contracting with the Company. Those vendors who do not meet the Company's baseline security requirements are not moved forward for procurement. Management reviews vendor security risk assessments every two years, or upon expansion or changes to the contracted service offering. Vendors deemed high risk, such as data center providers or other vendors storing or processing data in scope for the Company's regulatory or contractual requirements, undergo reassessment annually.

Internal Audit

mxHero follows the three lines of defense model established by the Institute of Internal Auditors, discussed in "The Three Lines of Defense in Effective Risk Management and Control" whitepaper. Per this model, management is the first layer of defense, various risk control and compliance oversight functions established by management are second, and independent assurance as needed is the third.

Given the size of the Company, and personnel resources, the Company contracts with Vanta, an independent third-party service provider, to provide internal audit services. While management of the Company is responsible for identifying risks and implementing appropriate controls to mitigate those risks, when necessary, Vanta monitors the operating effectiveness of implemented controls relevant to human resources, risk assessment, monitoring, logical access, system operations, and change management on a continuous basis. Vanta reports on the operating effectiveness of controls in real-time and sends alerts to management when exceptions are discovered. Management is responsible for responding appropriately for any discovered exception or deficiency.

Additionally, the Company works with a third-party assessor and undergoes an independent compliance examination (e.g., SOC 2®) on at least an annual basis.

The Applicable Trust Services Criteria

The Trust Services Categories that are in scope for the purposes of this report are as follows:

Security - Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the information or systems and affect mxHero's ability to meet its objectives.

The common criteria are organized as follows:

1. **Control environment** - The criteria relevant to how mxHero is structured and the processes mxHero has implemented to manage and support people within its operating units. This includes criteria addressing accountability, integrity, ethical values, and qualifications of personnel, and the environment in which they function.
2. **Communication and information** - The criteria relevant to how mxHero communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the System and the obligations of those parties and users to the effective operation of the System.
3. **Risk assessment** - The criteria relevant to how mxHero (i) identifies potential risks that would affect the mxHero's ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.
4. **Monitoring activities** - The criteria relevant to how mxHero monitors the System, including the suitability and design and operating effectiveness of the controls, and acts to address deficiencies identified.
5. **Control activities** - The criteria relevant to the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out.

6. **Logical and physical access controls** - The criteria relevant to how mxHero restricts logical and physical access, provides and removes that access, and prevents unauthorized access.
7. **System operations** - The criteria relevant to how mxHero manages the operation of system(s) and detects and mitigates processing deviations, including logical and physical security deviations.
8. **Change management** - The criteria relevant to how mxHero identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
9. **Risk mitigation** - The criteria relevant to how mxHero identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

Relevant Aspects of Internal Control

The control activities supporting the applicable Trust Services Criteria are included in Section IV of this report. Although the applicable Trust Services Criteria and related controls are included in Section IV, they are an integral part of the Company's description of its system.

Control Environment

Management Philosophy

mxHero's control environment reflects the philosophy of senior management concerning the importance of security of its services. Management meets weekly and reports to the board quarterly. Management, under the direction of the mxHero board, oversees the security activities of mxHero. Management is charged with establishing overall information security policies and procedures for mxHero. The importance of security is emphasized within mxHero through the establishment and communication of policies and procedures and is supported by investment in resources and people to carry out the policies. In designing its controls, mxHero has taken into consideration the relevance of controls to meet the relevant Trust Services Criteria.

Security Policies

The following information security policies and related processes are in place for the System:

- Data classification and business impact assessment
- Selection, documentation, and implementation of security controls
- Assessment of security controls
- User access authorization and provisioning
- Removal of user access
- Monitoring of security controls
- Security management

Jira is deployed to enhance the workflow and approval process in support of the policies. This application enables tracking of:

- Changes to data classification
- Additions, modifications, or deletions of users
- Changes to authority levels in access approvals

SECTION III - MXHERO'S DESCRIPTION OF ITS MAIL2CLOUD SYSTEM
THROUGHOUT THE PERIOD JULY 16, 2024 TO JULY 15, 2025

- Tests of new security components prior to installation
- Reviews of significant security monitoring events

Personnel Security

New employees are required to review and acknowledge their receipt of relevant information security policies. The new positions are supported by job descriptions. Once employed, employees are subject to mxHero's procedures for accessing systems and sanctions for violating mxHero's information security policies. Employees are instructed to report potential security incidents to the COO or CTO.

mxHero's business associate agreement instructs user entities to notify their respective account representative if they become aware of a possible security breach.

Physical Security and Environmental Controls

AWS is responsible for implementing and monitoring physical security controls for the data center(s) hosting the Company's production infrastructure. Management of the Company reviews AWS' most recent System and Organization Control (SOC) 2® report, which details the security measures in place, on at least an annual basis.

AWS employs UPS power systems, air conditioning systems, fire detection and suppression systems, and environmental monitoring and alert notification systems at the data center(s) hosting the Company's production infrastructure.

Risk Management

The Company recognizes that risk management is a critical component of its operations and contributes to ensuring customer data is properly protected. The Company incorporates risk management throughout its business processes and across the Company. The foundation of this process is management's knowledge of its operations, its close working relationship with its customers and vendors, and its understanding of the space in which it operates.

Management monitors the internal controls and conducts risk monitoring in accordance with relevant regulatory and contractual compliance requirements. This responsibility includes managing the design, implementation, and monitoring of the control environment, as well as assessing, monitoring, and mitigating security and compliance risks.

The Company's outsourced Internal Audit function identifies and prioritizes significant risks. The risk assessment incorporates input from multiple sources such as changes to the business, internal audits, operational events, and emerging risks.

Risk Identification and Mitigation

The Company has defined risk management processes to identify and manage risks that may affect the System's security. At least annually, management performs a risk assessment to identify and evaluate potential threats to the effectiveness of the control environment. This includes performing the following procedures:

- Classifying data into categories, listing examples of types of data within each category, and aligning policy with the data classifications.
- Incorporating various types of risks into the risk assessment process including but not limited to, Information Technology Risk, Business Risk, Organizational Risk, Vendor Risk, Fraud Risk and others.
- Maintains a thorough list of identified risks.
- Grades the risks for likelihood and impact.

SECTION III - MXHERO'S DESCRIPTION OF ITS MAIL2CLOUD SYSTEM
THROUGHOUT THE PERIOD JULY 16, 2024 TO JULY 15, 2025

- Tailors internal controls to mitigate risks to an acceptable level.
- Risk responses are selected for each identified risk. The responses fall into one of the four following categories:
 - Avoid: Risk avoidance involves changing aspects of the overall business process or system architecture to eliminate the threat.
 - Transfer: Risk transference involves shifting the negative impact of a threat (and ownership of the response) to a third party. Risk transference does not eliminate a threat it simply makes another party responsible for managing it. This would include identifying avenues of insurance, etc.
 - Mitigate: Risk mitigation involves reducing the probability and/or the impact of risk threat to an acceptable level. Taking early and pro-active action against a risk is often more effective than attempting to repair the damage a realized risk has caused. Developing contingency plans are examples of risk mitigation.
 - Accept: Risk acceptance should normally only be taken for low-priority risks. All risks should have a recommendation of control(s) and/or alternative solutions to mitigate risk.

Information and Communication

The Company has various IT policies such as the Information Security Policy to ensure that employees understand their individual roles and responsibilities concerning processing as well as controls to ensure that significant events are communicated in a timely manner. These policies include formal and informal training programs and the use of email and other mechanisms to communicate time-sensitive information and processes for security and system availability purposes that notify key personnel in the event of problems. Policies and supporting documents (and any changes to those documents) help users understand how the System relates to their roles and responsibilities and are communicated to all users.

The Company maintains a master services agreement and customer-specific service level agreements that communicate the Company's commitments, service provider responsibilities, and associated systems. Changes to any commitments are communicated to customers via the Company's website or in-application messaging.

The Company has also published documentation describing the security features of the service, internal security related processes and controls, and conformity to regulatory requirements. An overview of the Company's security processes is displayed on the Company's website at the following link: <https://www.mxhero.com/trust/>

The Company receives emails sent by the customers to the service for processing, given the nature of the product offered. However, the customer content is not retained once processed. The Company maintains documentation that describes the main categories of data that can be submitted by customers to the Company as part of the intended use of its product, and highlights scenarios where submitted data may contain personal data. Users can access the Company's product security documentation at the following link: <https://support.mxhero.com>

Monitoring

The systems within the boundary are configured to prevent and detect vulnerabilities. In addition to daily oversight and monthly reviews of logs and other usage of virtual infrastructure, management provides monitoring and audit logging in the form of preventive, detective, and corrective reporting. Relevant output from monitoring and detection mechanisms are distributed at monthly meetings with executive and management personnel. Security testing, both automated and manual, occurs at regular intervals. Third-party security experts perform vulnerability assessments and other security services more frequently than annually. Additionally, the Company has deployed anti-malware technology for environments commonly susceptible to malicious attack and has configured it to be updated routinely, logged, and installed on all relevant production servers.

Changes to the System During the Period

There were no changes that are likely to affect report users' understanding of how the System is used to provide the service during the period from July 16, 2024 through July 15, 2025.

System Incidents During the Period

There were no identified system incidents that were the result of controls that were not suitably designed or operating effectively or otherwise resulted in a significant failure in the achievement of one or more of the service commitments and system requirements during the period July 16, 2024 to July 15, 2025.

Complementary User Entity Controls (CUECs)

mxHero's controls related to the System cover only a portion of overall internal control for each user entity. It is not feasible for the criteria related to the System to be achieved solely by mxHero. Therefore, each user entity's internal controls should be evaluated in conjunction with mxHero's controls described in Section IV of this report, considering the related CUECs identified for the specific criterion. For user entities to rely on the controls reported herein, each user entity must evaluate its own internal control to determine whether the identified CUECs have been implemented and are operating effectively.

The user entity controls presented should not be regarded as a comprehensive list of all controls that should be employed by user entities. Management of user entities are responsible for the following:

Criteria	Complementary User Entity Controls
CC2.1	User entities are responsible for the security and integrity of data housed under user entity control, particularly the data utilized by mxHero systems and services.
CC6.1	User entities are responsible for determining what types of data and/or information, if any, should be protected when delivering via cloud storage, and how that information is protected within the scope of their cloud storage service offerings.
CC6.2	Determination of personnel who need specific functionality and the granting of such functionality is the responsibility of authorized personnel at the user entity. This includes allowing access to mxHero's application keys and API keys for access to the web service API.
CC6.3	Authorized users and their associated access are reviewed periodically.
CC6.6	User entities will ensure protective measures are in place for their data as it traverses from user entity to mxHero.
CC6.6	User entities should establish adequate physical security and environmental controls of all devices and access points residing at their operational facilities, including remote employees or at-home agents for which the user entity allows connectivity in order to provide authorized information to mxHero.

Subservice Organizations and Complementary Subservice Organization Controls (CSOCs)

mxHero utilizes AWS as a subservice organization for cloud hosting services. AWS is responsible for operating, managing, and controlling the components from the host operating system and storage, down to physical security and environmental controls over the facilities in which the services operate. AWS is examined annually in accordance with the *AICPA Guide, Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy (SOC 2®)*. This description and Section IV of this report include only the controls of the System and does not include any of the controls expected to be implemented at AWS.

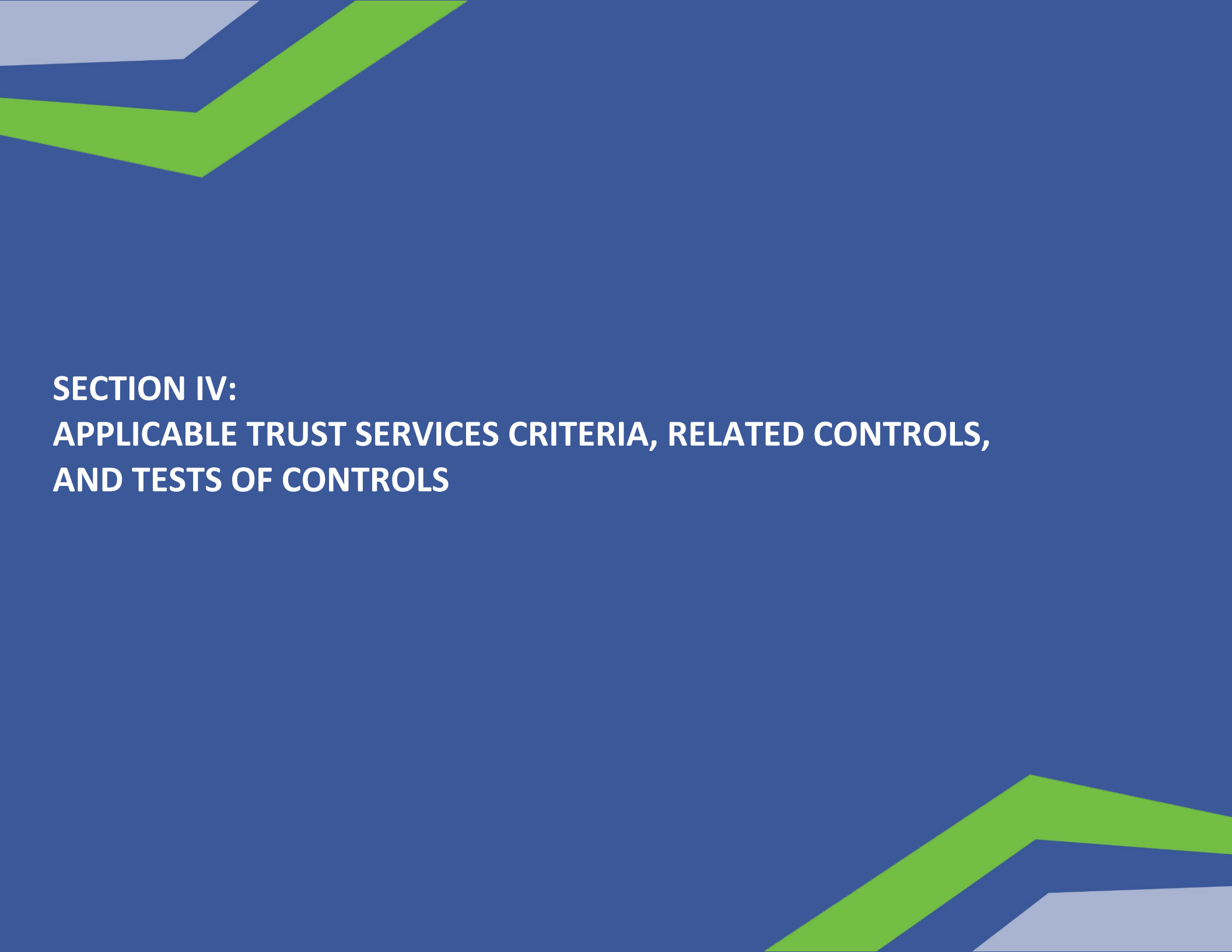
Although the subservice organization has been carved out for the purposes of this report, certain Trust Services Criteria are intended to be met by controls at the subservice organization. Management of mxHero receives and reviews the most recent SOC 2® reports available from AWS at least annually. In addition, through its operational activities, mxHero's management monitors the services performed by the subservice organization to determine whether operations and controls expected to be implemented at the subservice organization are functioning effectively. Management also has communication with the subservice organization to monitor compliance with service commitments, stay abreast of changes planned at the hosting facilities, and relay any issues or concerns to AWS management.

It is not feasible for the criteria related to the System to be achieved solely by mxHero. Therefore, each user entity's internal control must be evaluated in conjunction with mxHero's controls and related tests and results described in Section IV of this report, considering the related CSOCs expected to be implemented at the subservice organization as described below.

Criteria	Complementary Subservice Organization Controls Expected to be Implemented at AWS
CC2.3 CC7.3 CC7.4 CC7.5	AWS is responsible for notifying affected parties of security updates and/or identified security incidents.
CC6.4	AWS is responsible for restricting data center access to authorized personnel.
CC6.4	AWS is responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel.
CC6.5	AWS is responsible for the physical assets located within the data centers, including the secure decommissioning and physical destruction of production media prior to leaving AWS secure zones.
CC7.1	AWS is responsible for implementing a vulnerability management process that includes remediation of vulnerabilities in software, systems, and network devices.
CC7.2	AWS is responsible for the installation of fire suppression and detection, and environmental monitoring systems at the data centers.
CC7.2	AWS is responsible for protecting data centers against disruption in power supply to the processing environment by an uninterruptible power supply.
CC7.2	AWS is responsible for overseeing the regular maintenance of environmental protections at data centers.

Report Use

The description does not omit or distort information relevant to the System while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the System that each individual user may consider important to his or her own particular needs.

The slide features a solid blue background. In the top-left corner, there are overlapping geometric shapes in light blue and green. In the bottom-right corner, there are similar overlapping geometric shapes in green and light blue.

SECTION IV: APPLICABLE TRUST SERVICES CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS

SECTION IV - APPLICABLE TRUST SERVICES CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS
THROUGHOUT THE PERIOD JULY 16, 2024 TO JULY 15, 2025

Applicable Trust Services Criteria, Related Controls, and Tests of Controls

The applicable Trust Services Criteria, mxHero's related controls, and tests of controls are included in this section. For each criterion there is a control reference that leads the user to a description of the controls that are designed to meet the applicable Trust Services Criteria.

Tests of Controls

Tests applied to each control to test its operating effectiveness throughout the coverage period are listed alongside each control. Dansa D'Arata Soucia LLP deemed each test fit to provide reasonable assurance that the applicable Trust Services Criteria were achieved during the review period. In selecting each test of controls, Dansa D'Arata Soucia LLP considered the following factors:

- The nature of the control and the frequency with which it operates
- The control risk mitigated by the control
- The effectiveness of entity-level controls
- The degree to which the control relies on the effectiveness of other controls
- Whether the control is manually performed or automated

The types of tests performed with respect to operational effectiveness of the control activities detailed in this section are described below.

Type	Description
Inquiry	Inquired of personnel with related and appropriate level of skills, knowledge, and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of these means.
Observation	Observed the relevant processes and/or procedures during fieldwork. This included witnessing the performance of controls or evidence of control performance with the appropriate personnel, systems, or locations relevant to the performance of control policies and procedures.
Inspection	Inspected relevant audit support and the Company's records. This included, but was not limited to, documents, system configurations and settings, logs, as well as specific attributes such as signatures or approvals. In some instances, inspection involved tracing events forward or vouching backwards for preceding events.

SECTION IV - APPLICABLE TRUST SERVICES CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS
THROUGHOUT THE PERIOD JULY 16, 2024 TO JULY 15, 2025

Consistent with American Institute of Certified Public Accountants (AICPA) authoritative literature, Dansa D'Arata Soucia LLP utilizes professional judgement to consider the tolerable deviation rate, expected deviation rate, audit risk, characteristics of the population, and other factors in determining the number of items to be selected in a sample for a particular test. In accordance with AICPA authoritative literature, Dansa D'Arata Soucia LLP selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were maintained. In some instances, full populations were tested in cases including, but not limited to, the uniqueness of the event or the low overall population size.

Observation and inspection procedures were performed related to certain system-generated reports, listings, and queries to assess the accuracy and completeness of the information used in the performance of our testing of the controls.

Additionally, mxHero's internal audit function performed tests of controls for the following Trust Services Criteria: CC2.1, CC6.1, CC6.2, CC6.3, CC6.5, CC6.6, CC6.7, CC6.8, CC7.1, CC7.2, CC7.4, and CC8.1.

The tests performed by mxHero's internal audit function included inspection of technical configurations of relevant system components on a continuous basis. No deviations were noted by members of the internal audit function. We tested the work of the internal audit function through a combination of independent testing and review of the internal audit function's most recent SOC 2® report and noted no inconsistencies. The internal audit function's SOC 2® includes the Processing Integrity Trust Services Criteria in the scope of the report. Processing Integrity refers to the completeness, validity, accuracy, timeliness, and authorization of system processing in order to achieve the internal audit function's objectives. Processing integrity addresses whether systems achieve the aim or purpose for which they exist and whether they perform their intended functions in an unimpaired manner, free from error, delay, omission, and unauthorized or inadvertent manipulation.

Test Results

The results of each test are listed alongside each respective test applied to the control activity. Tests performed that yielded no deviations are noted by the phrase "No exceptions noted" in test results column. Testing deviations identified are not necessarily weaknesses in the total system of controls as this determination can only be made after considering controls in place at user entities and subservice organizations.

This report is intended solely for use by management of mxHero and the specified parties and is not intended and should not be used by anyone other than these parties.

SECTION IV - APPLICABLE TRUST SERVICES CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS
THROUGHOUT THE PERIOD JULY 16, 2024 TO JULY 15, 2025

Control Environment		
CC1.1 - The entity demonstrates a commitment to integrity and ethical values.		
Control	Control Test Performed by Auditor	Test Result(s)
The Company requires employees to acknowledge a code of conduct at the time of hire, and as the Company updates its policies. The Company's code of conduct applies to all business and non-business activities that may adversely affect the safety and well-being of the Company or the Company's customers. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.	Inspected policy acknowledgements for all relevant employees to verify they had agreed to the Company's most recent version of its Code of Conduct, Acceptable Use Policy, and Human Resource Security Policy. Inspected the Company's records to verify a policy that establishes the acceptable use of information assets is in place, has been approved by management, and is accessible to employees. Inspected the policy that documents the Company's Code of Conduct to verify it provides guidance on reporting violations to members of leadership.	No exceptions noted.
Contractor agreements include a code of conduct or reference to the Company's Code of Conduct.	Inspected policy acknowledgements for all relevant contractors to verify they had agreed to the Company's most recent version of its Code of Conduct. Inspected the Company's standard contractor agreement to verify it requires newly onboarded contractors to acknowledge receipt of the Company's Code of Conduct. Inspected the Company's records to verify newly onboarded contractors executed a formal contractor agreement upon hire.	No exceptions noted. No exceptions noted. Per inspection of the Company's records, no new contractors were hired during the examination period. As such, we are unable to test the Company's contractor onboarding procedures.
Employees and contractors are required to sign a confidentiality agreement at time of hire which prohibits the disclosure of confidential information to unauthorized parties.	Inspected the Company's standard confidentiality agreement to verify it prohibits the disclosure of confidential information to unauthorized parties. Inspected signed confidentiality agreements for a sample of employees and contractors onboarded during the examination period to verify they had agreed to the Company's confidentiality policy upon hire.	No exceptions noted. Per inspection of the Company's records, no new employees or contractors were hired during the examination period. As such, we are unable to test the Company's onboarding procedures.
The Company managers are required to complete performance evaluations for direct reports at least annually.	Inspected the Company's process for formal performance evaluations to verify they describe a formal process to evaluate employee competency. Inspected a sample of completed performance evaluations to verify they were conducted in the prior 12 months.	No exceptions noted.
The Company performs background checks on new employees.	Inspected the Company's records to verify that a background investigation was performed on newly hired employees, as permitted by local laws.	Per inspection of the Company's records, there were no new employees hired during the examination period. As such, we were unable to test the Company's background check procedures.

SECTION IV - APPLICABLE TRUST SERVICES CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS
THROUGHOUT THE PERIOD JULY 16, 2024 TO JULY 15, 2025

CC1.2 - The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.		
Control	Control Test Performed by Auditor	Test Result(s)
The board of directors is briefed by senior management at least annually on the state of the Company's cyber and privacy risk. Briefings may include: - Information Security Policy changes and updates - Updates on performance of the information security and privacy program or management system - Results of risk assessments and technical tests - Status of risk treatment plans - Results of internal control audits - Material changes in staffing or controls The board provides feedback and direction to management as needed.	Inquired of management as to who is responsible for governing the Company, and what responsibilities they have, to verify the functioning of internal control is monitored by the appropriate personnel. Inspected board meeting minutes to verify discussions were held during the examination period.	No exceptions noted.
Board members have sufficient expertise to oversee management's ability to design, implement and operate information security controls. The board engages third-party information security experts and consultants as needed.	Inspected professional backgrounds of board members and external advisors, as necessary, to verify they have appropriate skills, knowledge, and experience as it relates to information security.	No exceptions noted.
The board of directors meets at least annually and maintains formal meeting minutes. The board includes directors that are independent of the Company.	Inspected board meeting minutes to verify discussions were held during the examination period.	No exceptions noted.
CC1.3 - Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.		
Control	Control Test Performed by Auditor	Test Result(s)
The board of directors is briefed by senior management at least annually on the state of the Company's cyber and privacy risk. Briefings may include: - Information Security Policy changes and updates - Updates on performance of the information security and privacy program or management system - Results of risk assessments and technical tests - Status of risk treatment plans - Results of internal control audits - Material changes in staffing or controls The board provides feedback and direction to management as needed.	Inquired of management as to who is responsible for governing the Company, and what responsibilities they have, to verify the functioning of internal control is monitored by the appropriate personnel. Inspected board meeting minutes to verify discussions were held during the examination period.	No exceptions noted.
Management has established defined roles and responsibilities to oversee the implementation of information security controls.	Inspected policy acknowledgements for all relevant employees to verify they had agreed to the Company's most recent version of its Information Security Policy. Inspected the Company's Information Security Policy to verify that it describes, assigns, and communicates the Security Officer Role within the Company.	No exceptions noted.
Job descriptions for relevant employees include authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls.	Inspected a sample engineering job description to verify qualifications to be hired are established. Inspected the Company's Information Security Roles and Responsibilities Policy to verify qualifications to be hired are established.	No exceptions noted.

SECTION IV - APPLICABLE TRUST SERVICES CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS
THROUGHOUT THE PERIOD JULY 16, 2024 TO JULY 15, 2025

An organizational chart describes the organizational structure and reporting lines.	Inspected the Company's organizational chart to verify that the organizational chart clearly defines lines of communication and are accessible to employees.	No exceptions noted.
CC1.4 - The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.		
Control	Control Test Performed by Auditor	Test Result(s)
Employees complete security awareness training upon hire and annually thereafter.	Inspected the security awareness training that all employees must complete to verify that it provides information related to the tactics that hackers take that could compromise the security of the Company and its customers' data. Inspected the Company's records to verify all relevant employees completed security awareness training in the previous 12 months.	No exceptions noted.
Job descriptions for relevant employees include authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls.	Inspected a sample engineering job description to verify qualifications to be hired are established. Inspected the Company's Information Security Roles and Responsibilities Policy to verify qualifications to be hired are established.	No exceptions noted.
The Company managers are required to complete performance evaluations for direct reports at least annually.	Inspected the Company's process for formal performance evaluations to verify they describe a formal process to evaluate employee competency. Inspected a sample of completed performance evaluations to verify they were conducted in the prior 12 months.	No exceptions noted.
The Company performs background checks on new employees.	Inspected the Company's records to verify that a background investigation was performed on newly hired employees, as permitted by local laws.	Per inspection of the Company's records, there were no new employees hired during the examination period. As such, we were unable to test the Company's background check procedures.
CC1.5 - The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.		
Control	Control Test Performed by Auditor	Test Result(s)
The Company managers are required to complete performance evaluations for direct reports at least annually.	Inspected the Company's process for formal performance evaluations to verify they describe a formal process to evaluate employee competency. Inspected a sample of completed performance evaluations to verify they were conducted in the prior 12 months.	No exceptions noted.
The Company requires employees to acknowledge a code of conduct at the time of hire, and as the Company updates its policies. The Company's code of conduct applies to all business and non-business activities that may adversely affect the safety and well-being of the Company or the Company's customers. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.	Inspected policy acknowledgements for all relevant employees to verify they had agreed to the Company's most recent version of its Code of Conduct, Acceptable Use Policy, and Human Resource Security Policy. Inspected the Company's records to verify a policy that establishes the acceptable use of information assets is in place, has been approved by management, and is accessible to employees. Inspected the policy that documents the Company's Code of Conduct to verify it provides guidance on reporting violations to members of leadership.	No exceptions noted.

SECTION IV - APPLICABLE TRUST SERVICES CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS
THROUGHOUT THE PERIOD JULY 16, 2024 TO JULY 15, 2025

The Company management annually evaluates roles and responsibilities for pressures associated with the achievement of security objectives and makes adjustments to roles, responsibilities, performance evaluation, or performance measures as needed.	Inspected policy acknowledgements for all relevant employees to verify they had agreed to the Company's most recent version of its Human Resource Security Policy and Information Security Policy. Inspected a sample engineering job description to verify qualifications to be hired are established. Inspected the Company's process for formal performance evaluations to verify they describe a formal process to evaluate employee competency.	No exceptions noted.
Job descriptions for relevant employees include authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls.	Inspected a sample engineering job description to verify qualifications to be hired are established. Inspected the Company's Information Security Roles and Responsibilities Policy to verify qualifications to be hired are established.	No exceptions noted.
Communication and Information		
CC2.1 - The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.		
Control	Control Test Performed by Auditor	Test Result(s)
Control self-assessments are performed by the Company at least annually to gain assurance that controls related to the in-scope Trust Services Categories (TSCs) are in place and operating effectively. These assessments are done using a tool called Vanta which objectively and continuously monitors company control environment and alerts management when internal control and security issues arise. Corrective actions are taken based on relevant findings and tracked to resolution.	Inspected the Company's GRC tool to verify they use it to continuously monitor the Company's control environment, it sends alerts for control shortfalls in real time, and corrective actions are taken and tracked to resolution.	No exceptions noted.
Vulnerability scans are performed continuously. A remediation plan is developed and changes are implemented to remediate all critical and high vulnerabilities, at a minimum, within a specified SLA.	Inspected the configuration for the tool that monitors infrastructure packages to verify that it is active and alerts on vulnerabilities. Inspected alerts generated by the infrastructure-package vulnerability scanner to verify they're addressed within a specified SLA. Inspected the Company's task tracker and confirmed security issues are tracked in a shared issue tracking system.	No exceptions noted.
A log management tool is utilized to identify trends that may have a potential impact on the Company's ability to achieve its security objectives.	Inspected the configuration of AWS to verify that all VPCs have flow logs enabled and no S3 logging buckets grant access to the built-in AWS groups. Inspected the configuration of AWS to verify that all linked accounts have CloudTrail enabled and at least one S3 bucket acting as a destination for server access logging or CloudTrail data event logging. Inspected the configuration of AWS to verify that all CloudWatch Log Groups are configured to retain logs for at least 365 days. Inspected the configuration of AWS to verify that all audit log types are enabled for your AWS EKS clusters.	No exceptions noted.

SECTION IV - APPLICABLE TRUST SERVICES CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS
THROUGHOUT THE PERIOD JULY 16, 2024 TO JULY 15, 2025

The security owner subscribes to industry security bulletins and email alerts and uses them to monitor the impact of emerging technologies and security.	Inspected the Company's records to verify security owner subscribes to industry security bulletins and email alerts.	No exceptions noted.
The Company has a Data Management Policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the Company's Data Management Policy to verify that it is in place and includes policies for the storage and use of confidential data. Inspected policy acknowledgements for all relevant employees to verify they had agreed to the Company's most recent version of its Data Management Policy.	No exceptions noted.
The Company maintains a formal inventory of production system assets. Assets are classified by type, owners, location, and type(s) of data accessed by the asset.	Inspected an inventory listing of information assets the Company maintains in order to protect inventory from security events to verify assets are labeled and categorized appropriately.	No exceptions noted.
CC2.2 - The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.		
Control	Control Test Performed by Auditor	Test Result(s)
Incident response policies and procedures are documented and communicated to authorized users.	Inspected policy acknowledgements for all relevant employees to verify they had agreed to the Company's most recent version of its Incident Response Plan. Inspected the Incident Response Plan to verify that it included a section about tracking follow-ups after incidents, writing lessons learned documents after incidents, outlines formal procedure for responding to security events, and names the individuals responsible for monitoring for and responding to incidents.	No exceptions noted.
The Company's Code of Conduct establishes an appropriate communication channel for employees to report potential security issues or fraud concerns.	Inspected the Company's Code of Conduct to verify it details a process for employees to report failures, incidents, and concerns.	No exceptions noted.
Information security policies and procedures are documented and define the information security rules and requirements for the service environment. These policies and procedures are reviewed by the Company at least annually and updated as needed.	Inspected the Company's information security policies to verify they define the information security rules and requirements for the service environment. Inspected policy acknowledgements for all relevant employees to verify they had agreed to the Company's information security policies and procedures. Inspected the Company's records to verify that management reviews and approves the policies at least annually, or when business objectives and/or strategies significantly change.	No exceptions noted.
The Company provides a description of its products and services to internal and external users. Information requirements necessary to use the System are communicated.	Inspected the Company's URL to an external product page and customer support page on their website to verify it is available to both internal and external users.	No exceptions noted.
System changes are communicated to authorized internal users.	Inspected a sample of communications sent to the product, engineering, support, marketing, or sales teams when product or system changes took place to verify they were sent within an appropriate amount of time and to the appropriate personnel.	No exceptions noted.
Employees complete security awareness training upon hire and annually thereafter.	Inspected the security awareness training that all employees must complete to verify that it provides information related to the tactics that hackers take that could compromise the security of the Company and its customers' data. Inspected the Company's records to verify all relevant employees completed security awareness training in the previous 12 months.	No exceptions noted.

SECTION IV - APPLICABLE TRUST SERVICES CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS
THROUGHOUT THE PERIOD JULY 16, 2024 TO JULY 15, 2025

Management has established defined roles and responsibilities to oversee the implementation of information security controls.	Inspected policy acknowledgements for all relevant employees to verify they had agreed to the Company's most recent version of its Information Security Policy. Inspected the Company's Information Security Policy to verify that it describes, assigns, and communicates the Security Officer Role within the Company.	No exceptions noted.
Job descriptions for relevant employees include authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls.	Inspected a sample engineering job description to verify qualifications to be hired are established. Inspected the Company's Information Security Roles and Responsibilities Policy to verify qualifications to be hired are established.	No exceptions noted.
CC2.3 - The entity communicates with external parties regarding matters affecting the functioning of internal control.		
Control	Control Test Performed by Auditor	Test Result(s)
The Company's security commitments are communicated to customers in SaaS Agreements or Terms of Service (TOS).	Inspected the Company's SaaS Agreement and TOS to verify their security commitments are communicated to their customers. Inspected a sample of executed SaaS Agreements to verify customers onboarded during the examination period agreed to the Company's SaaS Agreement. Inspected the Company's website to verify the TOS is accessible and provided to their customers.	No exceptions noted.
The Company has written agreements in place with vendors and related third-parties.	Inspected the vendor list to verify that the Company maintains a complete list of vendors. Inspected a sample of executed vendor agreements to verify executed agreements are in place between the Company and its vendors.	No exceptions noted.
An external-facing support system is in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.	Inspected URL made available to external users of the System to verify it links to a support system. Inspected a sample of customer support tickets to verify they are tracked to completion.	No exceptions noted.
Customers are notified of critical changes that may affect their processing.	Inspected the Company's URL to their customer accessible support page where support contact information is readily available. Further verified customers and/or associated users are encouraged to contact appropriate company personnel if they become aware of items such as operational or security failures, incidents, system problems, concerns, or other complaints. Inspected the Company's public release notes to verify product updates are communicated to users.	No exceptions noted.
The Company provides guidelines and technical support resources relating to system operations to customers.	Inspected URL made available to external users of the System to verify it links to a technical support page.	No exceptions noted.
The Company provides a description of its products and services to internal and external users. Information requirements necessary to use the System are communicated.	Inspected the Company's URL to an external product page and customer support page on their website to verify it is available to both internal and external users.	No exceptions noted.
Criteria also addressed via subservice provider controls.		

SECTION IV - APPLICABLE TRUST SERVICES CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS
THROUGHOUT THE PERIOD JULY 16, 2024 TO JULY 15, 2025

Risk Assessment		
CC3.1 - The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.		
Control	Control Test Performed by Auditor	Test Result(s)
The Company specifies its objectives in its risk assessment to enable the identification and assessment of risk related to the objectives.	Inspected the security risk assessment, which includes the risks, prioritization, and resulting action plans to verify it is documented in a risk register.	No exceptions noted.
The Company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the Company's Risk Management Policy to verify there is a formal program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
Risk assessments are performed by the Company at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the Company's Risk Management Policy to verify there is a formal program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. Inspected the security risk assessment, which includes the risks, prioritization, and resulting action plans to verify it is documented in a risk register.	No exceptions noted.
The Company maintains a formal inventory of production system assets. Assets are classified by type, owners, location, and type(s) of data accessed by the asset.	Inspected an inventory listing of information assets the Company maintains in order to protect inventory from security events to verify assets are labeled and categorized appropriately.	No exceptions noted.
CC3.2 - The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.		
Control	Control Test Performed by Auditor	Test Result(s)
Risk assessments are performed by the Company at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the Company's Risk Management Policy to verify there is a formal program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. Inspected the security risk assessment, which includes the risks, prioritization, and resulting action plans to verify it is documented in a risk register.	No exceptions noted.
The Company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the Company's Risk Management Policy to verify there is a formal program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
A vendor management program is in place. Components of this program include: - Maintaining a list of critical third-party vendors. - Monitoring and reviewing service delivery. - Requirements for third-party vendors to maintain their own security practices and procedures. - Annually reviewing critical third-party attestation reports or performing a vendor risk assessment.	Inspected the Company's Third-Party Management Policy to verify that the Company provides a process for documenting and managing vendor relationships through maintaining a list of vendors, requirements for third-party vendors to maintain their own security practices and procedures, and annually reviewing critical third-party attestation reports or performing a vendor risk assessment.	No exceptions noted.
The Company maintains a formal inventory of production system assets. Assets are classified by type, owners, location, and type(s) of data accessed by the asset.	Inspected an inventory listing of information assets the Company maintains in order to protect inventory from security events to verify assets are labeled and categorized appropriately.	No exceptions noted.

SECTION IV - APPLICABLE TRUST SERVICES CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS
THROUGHOUT THE PERIOD JULY 16, 2024 TO JULY 15, 2025

Business Continuity and Disaster Recovery plans are in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.	Inspected the Company's Business Continuity Plan to verify it defines an operational and organizational strategy in the event of a disruption and has been updated in the past year. Inspected the Company's Disaster Recovery Plan to verify that it outlines steps to take in the event of a disaster and has been updated in the past year.	No exceptions noted.
CC3.3 - The entity considers the potential for fraud in assessing risks to the achievement of objectives.		
Control	Control Test Performed by Auditor	Test Result(s)
The Company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the Company's Risk Management Policy to verify there is a formal program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
Risk assessments are performed by the Company at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the Company's Risk Management Policy to verify there is a formal program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. Inspected the security risk assessment, which includes the risks, prioritization, and resulting action plans to verify it is documented in a risk register.	No exceptions noted.
The Company maintains a formal inventory of production system assets. Assets are classified by type, owners, location, and type(s) of data accessed by the asset.	Inspected an inventory listing of information assets the Company maintains in order to protect inventory from security events to verify assets are labeled and categorized appropriately.	No exceptions noted.
CC3.4 - The entity identifies and assesses changes that could significantly impact the System of internal control.		
Control	Control Test Performed by Auditor	Test Result(s)
Risk assessments are performed by the Company at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the Company's Risk Management Policy to verify there is a formal program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. Inspected the security risk assessment, which includes the risks, prioritization, and resulting action plans to verify it is documented in a risk register.	No exceptions noted.
The Company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the Company's Risk Management Policy to verify there is a formal program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
Business Continuity and Disaster Recovery plans are in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.	Inspected the Company's Business Continuity Plan to verify it defines an operational and organizational strategy in the event of a disruption and has been updated in the past year. Inspected the Company's Disaster Recovery Plan to verify that it outlines steps to take in the event of a disaster and has been updated in the past year.	No exceptions noted.

SECTION IV - APPLICABLE TRUST SERVICES CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS
THROUGHOUT THE PERIOD JULY 16, 2024 TO JULY 15, 2025

Penetration testing is performed at least annually. A remediation plan is developed and changes are implemented by the Company to remediate all critical and high vulnerabilities or findings at a minimum.	Inspected the report from the Company's latest penetration test to verify it was performed in the previous 12 months. Additionally, verified that all critical and high-priority findings were remediated as needed.	No exceptions noted.
The Company maintains a formal inventory of production system assets. Assets are classified by type, owners, location, and type(s) of data accessed by the asset.	Inspected an inventory listing of information assets the Company maintains in order to protect inventory from security events to verify assets are labeled and categorized appropriately.	No exceptions noted.
Monitoring Activities		
CC4.1 - The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.		
Control	Control Test Performed by Auditor	Test Result(s)
Control self-assessments are performed by the Company at least annually to gain assurance that controls related to the in-scope Trust Services Categories (TSCs) are in place and operating effectively. These assessments are done using a tool called Vanta which objectively and continuously monitors company control environment and alerts management when internal control and security issues arise. Corrective actions are taken based on relevant findings and tracked to resolution.	Inspected the Company's GRC tool to verify they use it to continuously monitor the Company's control environment, it sends alerts for control shortfalls in real time, and corrective actions are taken and tracked to resolution.	No exceptions noted.
A vendor management program is in place. Components of this program include: - Maintaining a list of critical third-party vendors. - Monitoring and reviewing service delivery. - Requirements for third-party vendors to maintain their own security practices and procedures. - Annually reviewing critical third-party attestation reports or performing a vendor risk assessment.	Inspected the Company's Third-Party Management Policy to verify that the Company provides a process for documenting and managing vendor relationships through maintaining a list of vendors, requirements for third-party vendors to maintain their own security practices and procedures, and annually reviewing critical third-party attestation reports or performing a vendor risk assessment.	No exceptions noted.
Penetration testing is performed at least annually. A remediation plan is developed and changes are implemented by the Company to remediate all critical and high vulnerabilities or findings at a minimum.	Inspected the report from the Company's latest penetration test to verify it was performed in the previous 12 months. Additionally, verified that all critical and high-priority findings were remediated as needed.	No exceptions noted.
Vulnerability scans are performed continuously. A remediation plan is developed and changes are implemented to remediate all critical and high vulnerabilities, at a minimum, within a specified SLA.	Inspected the configuration for the tool that monitors infrastructure packages to verify that it is active and alerts on vulnerabilities. Inspected alerts generated by the infrastructure-package vulnerability scanner to verify they're addressed within a specified SLA. Inspected the Company's task tracker and confirmed security issues are tracked in a shared issue tracking system.	No exceptions noted.
CC4.2 - The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.		
Control	Control Test Performed by Auditor	Test Result(s)
A vendor management program is in place. Components of this program include: - Maintaining a list of critical third-party vendors. - Monitoring and reviewing service delivery. - Requirements for third-party vendors to maintain their own security practices and procedures. - Annually reviewing critical third-party attestation reports or performing a vendor risk assessment.	Inspected the Company's Third-Party Management Policy to verify that the Company provides a process for documenting and managing vendor relationships through maintaining a list of vendors, requirements for third-party vendors to maintain their own security practices and procedures, and annually reviewing critical third-party attestation reports or performing a vendor risk assessment.	No exceptions noted.

SECTION IV - APPLICABLE TRUST SERVICES CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS
THROUGHOUT THE PERIOD JULY 16, 2024 TO JULY 15, 2025

Control self-assessments are performed by the Company at least annually to gain assurance that controls related to the in-scope Trust Services Categories (TSCs) are in place and operating effectively. These assessments are done using a tool called Vanta which objectively and continuously monitors company control environment and alerts management when internal control and security issues arise. Corrective actions are taken based on relevant findings and tracked to resolution.	Inspected the Company's GRC tool to verify they use it to continuously monitor the Company's control environment, it sends alerts for control shortfalls in real time, and corrective actions are taken and tracked to resolution.	No exceptions noted.
Control Activities		
CC5.1 - The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.		
Control	Control Test Performed by Auditor	Test Result(s)
Information security policies and procedures are documented and define the information security rules and requirements for the service environment. These policies and procedures are reviewed by the Company at least annually and updated as needed.	Inspected the Company's information security policies to verify they define the information security rules and requirements for the service environment. Inspected policy acknowledgements for all relevant employees to verify they had agreed to the Company's information security policies and procedures. Inspected the Company's records to verify that management reviews and approves the policies at least annually, or when business objectives and/or strategies significantly change.	No exceptions noted.
The Company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the Company's Risk Management Policy to verify there is a formal program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC5.2 - The entity also selects and develops general control activities over technology to support the achievement of objectives.		
Control	Control Test Performed by Auditor	Test Result(s)
Formal procedures are documented that outline the process the Company's staff follows to perform the following access control functions: - Adding new users - Modifying an existing user's access - Removing an existing user's access	Inspected the Company's security policies to verify that they require that employees may only access the customer data they need in order to complete their jobs. Inspected policy acknowledgements for all relevant employees to verify they had agreed to the Company's most recent version of its Access Control Policy. Inspected policy acknowledgements for all relevant employees to verify they had agreed to the Company's most recent version of its Information Security Roles and Responsibilities Policy.	No exceptions noted.
Information security policies and procedures are documented and define the information security rules and requirements for the service environment. These policies and procedures are reviewed by the Company at least annually and updated as needed.	Inspected the Company's information security policies to verify they define the information security rules and requirements for the service environment. Inspected policy acknowledgements for all relevant employees to verify they had agreed to the Company's information security policies and procedures. Inspected the Company's records to verify that management reviews and approves the policies at least annually, or when business objectives and/or strategies significantly change.	No exceptions noted.

SECTION IV - APPLICABLE TRUST SERVICES CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS
THROUGHOUT THE PERIOD JULY 16, 2024 TO JULY 15, 2025

A formal systems development life cycle (SDLC) methodology is in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the Company's Secure Development Policy and Operations Security Policy to verify that it outlines considerations for planning, design, security, availability, implementation, and maintenance of changes.	No exceptions noted.
CC5.3 - The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.		
Control	Control Test Performed by Auditor	Test Result(s)
The Company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected the configuration of the version control system and/or tickets in the task tracker to verify that production changes must be reviewed and approved by an independent technical resource prior to deployment to production. Inspected tickets from the version control system and task tracker to verify that production changes are tested, reviewed, and approved prior to being implemented in the production environment. Inspected tickets from the version control system and task tracker to verify that production changes are evaluated for their potential effect on the Company's security commitments.	No exceptions noted.
Formal procedures are documented that outline the process the Company's staff follows to back up and recover customer data.	Inspected the Company's security policies to verify they outline requirements for backup and recovery of customer data. Inspected documentation from a backup-recovery tabletop exercise to verify that critical data could be quickly restored from a backup if necessary. Inspected the configuration of databases used in production to verify they are backed up on a continuous basis.	No exceptions noted.
Incident response policies and procedures are documented and communicated to authorized users.	Inspected policy acknowledgements for all relevant employees to verify they had agreed to the Company's most recent version of its Incident Response Plan. Inspected the Incident Response Plan to verify that it included a section about tracking follow-ups after incidents, writing lessons learned documents after incidents, outlines formal procedure for responding to security events, and names the individuals responsible for monitoring for and responding to incidents.	No exceptions noted.
Information security policies and procedures are documented and define the information security rules and requirements for the service environment. These policies and procedures are reviewed by the Company at least annually and updated as needed.	Inspected the Company's information security policies to verify they define the information security rules and requirements for the service environment. Inspected policy acknowledgements for all relevant employees to verify they had agreed to the Company's information security policies and procedures. Inspected the Company's records to verify that management reviews and approves the policies at least annually, or when business objectives and/or strategies significantly change.	No exceptions noted.
The Company specifies its objectives in its risk assessment to enable the identification and assessment of risk related to the objectives.	Inspected the security risk assessment, which includes the risks, prioritization, and resulting action plans to verify it is documented in a risk register.	No exceptions noted.

**SECTION IV - APPLICABLE TRUST SERVICES CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS
THROUGHOUT THE PERIOD JULY 16, 2024 TO JULY 15, 2025**

Job descriptions for relevant employees include authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls.	Inspected a sample engineering job description to verify qualifications to be hired are established. Inspected the Company's Information Security Roles and Responsibilities Policy to verify qualifications to be hired are established.	No exceptions noted.
The Company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the Company's Risk Management Policy to verify there is a formal program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
A formal systems development life cycle (SDLC) methodology is in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the Company's Secure Development Policy and Operations Security Policy to verify that it outlines considerations for planning, design, security, availability, implementation, and maintenance of changes.	No exceptions noted.
A vendor management program is in place. Components of this program include: - Maintaining a list of critical third-party vendors. - Monitoring and reviewing service delivery. - Requirements for third-party vendors to maintain their own security practices and procedures. - Annually reviewing critical third-party attestation reports or performing a vendor risk assessment.	Inspected the Company's Third-Party Management Policy to verify that the Company provides a process for documenting and managing vendor relationships through maintaining a list of vendors, requirements for third-party vendors to maintain their own security practices and procedures, and annually reviewing critical third-party attestation reports or performing a vendor risk assessment.	No exceptions noted.
Formal retention and disposal procedures are in place to guide the secure retention and disposal of company and customer data.	Inspected the Data Management Policy to verify that data retention and disposal procedures were documented to guide the secure retention and disposal of company and customer data.	No exceptions noted.
Logical and Physical Access Controls		
CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.		
Control	Control Test Performed by Auditor	Test Result(s)
Privileged access to the production network, application, operating system, and databases are restricted to authorized users with a business need.	Inspected the cloud provider to verify that all accounts are actively monitored by the Company's GRC tool. Inspected configurations on relevant software (i.e. Infrastructure, email, version control, chat) to verify that all employees have unique usernames. Inspected configurations on the Company's infrastructure to verify that all employees have unique usernames. Additionally, verified that the root infrastructure account is not being used, all accounts are assigned to a group, and roles are assigned at the group level. Lastly, reviewed inactive accounts to verify that all inactive accounts that have not been disabled have been inactive for less than 90 days. Inspected termination checklists to verify that terminated employees' accounts were removed from critical systems within the specified SLA of the employee becoming unauthorized.	No exceptions noted.

SECTION IV - APPLICABLE TRUST SERVICES CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS
THROUGHOUT THE PERIOD JULY 16, 2024 TO JULY 15, 2025

Privileged access to encryption keys is restricted to authorized users with a business need.	Inspected the Company's Cryptography Policy to verify they explain the procedures for encrypting sensitive data and access to encryption keys is restricted. Inspected access lists for the infrastructure provider to verify that access is limited to authorized personnel and must be approved by an existing administrator.	No exceptions noted.
User access to system components is based on job role and function and requires a documented access request form and manager approval prior to access being provisioned.	Inspected policy acknowledgements for all relevant employees to verify they had agreed to the Company's most recent version of its Access Control Policy. Inspected a sample of access request tickets to verify user access follows the Company's Access Control Policy.	No exceptions noted. Per inquiry of management, there were no access request tickets within the examination period. As such, we were unable to test the Company's access request procedures.
Privileged access to the firewall is restricted to authorized users with a business need.	Inspected the configuration of the Company's laptops to verify that no two workstations share SSH keys if the workstations are owned by different users. Inspected the cloud provider configuration to verify all AWS EC2 instances have security groups configured to restrict inbound SSH (TCP port 22) traffic from the public internet (0.0.0.0/0). Inspected the configuration of AWS to verify that all EC2 instances have network ACLs or security groups attached. Inspected the configuration of AWS to verify that each RDS instance's attached Security Groups are only accessible by restricted IP addresses.	No exceptions noted.
Authentication to company systems, applications, and datastores uses unique username and password or authorized Secure Socket Shell (SSH) keys.	Inspected the configuration of the Company's laptops to verify that no two workstations share SSH keys if the workstations are owned by different users. Inspected configuration of the Company's identity provider, version control system, and infrastructure to verify all users have MFA enabled. Inspected the configuration of the Company's identity and access management tool to verify that a password policy was applied to each user. Inspected configurations of AWS to verify that all employees/contractors have unique usernames. Additionally, verified that the root infrastructure account is not being used, all accounts are assigned to a group, and roles are assigned at the group level. Lastly, reviewed inactive accounts to verify that all inactive accounts that have not been disabled have been inactive for less than 90 days.	No exceptions noted.
The Company maintains a formal inventory of production system assets. Assets are classified by type, owners, location, and type(s) of data accessed by the asset.	Inspected an inventory listing of information assets the Company maintains in order to protect inventory from security events to verify assets are labeled and categorized appropriately.	No exceptions noted.

SECTION IV - APPLICABLE TRUST SERVICES CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS
THROUGHOUT THE PERIOD JULY 16, 2024 TO JULY 15, 2025

Formal procedures are documented that outline the process the Company's staff follows to perform the following access control functions: - Adding new users - Modifying an existing user's access - Removing an existing user's access	Inspected the Company's security policies to verify that they require that employees may only access the customer data they need in order to complete their jobs. Inspected policy acknowledgements for all relevant employees to verify they had agreed to the Company's most recent version of its Access Control Policy. Inspected policy acknowledgements for all relevant employees to verify they had agreed to the Company's most recent version of its Information Security Roles and Responsibilities Policy.	No exceptions noted.
The network is segmented to prevent unauthorized access to customer data.	Inspected the diagram of the Company's in-scope network to verify it accurately reflected the Company's in-scope network and there is appropriate segmentation. Inspected the VPC and router configuration to verify that access control lists were used to filter unwanted network traffic.	No exceptions noted.
Passwords for in-scope system components are configured according to the Company's policy.	Inspected the MDM tool to verify that the Company's employee computers are running a password manager. Inspected the configuration of the infrastructure provider's identity and access management tool to verify that a password policy was applied to each user and required minimum length and types of characters used.	No exceptions noted.
Access to migrate changes to production is restricted to authorized personnel.	Inspected the Company's version control system to verify that at least one approval is required to merge to the default branch for all production repositories. Inspected all user accounts with access to the version control system to verify that each is configured with MFA. Inspected the Company's version control system to verify that the visibility of all repositories has been set to private. Inspected the Company's version control system to verify that at least one production repository has been updated in the last 30 days. Inspected policy acknowledgements for all relevant employees to verify they had agreed to the Company's most recent version of its Operations Security Policy and Secure Development Policy.	No exceptions noted.
Data stores housing sensitive customer data are encrypted at rest.	Inspected the configuration of AWS to verify that DynamoDB Tables are encrypted at rest. Inspected the configuration of AWS to verify that Amazon RDS instances are encrypted at rest.	No exceptions noted.
Production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) token.	Inspected all user accounts with access to the infrastructure, the infrastructure root account, identity provider users, and the version control system to verify that each is configured with MFA.	No exceptions noted.

SECTION IV - APPLICABLE TRUST SERVICES CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS
THROUGHOUT THE PERIOD JULY 16, 2024 TO JULY 15, 2025

The Company has a Data Management Policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the Company's Data Management Policy to verify that it is in place and includes policies for the storage and use of confidential data. Inspected policy acknowledgements for all relevant employees to verify they had agreed to the Company's most recent version of its Data Management Policy.	No exceptions noted.
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.		
Control	Control Test Performed by Auditor	Test Result(s)
Authentication to company systems, applications, and datastores uses unique username and password or authorized Secure Socket Shell (SSH) keys.	Inspected the configuration of the Company's laptops to verify that no two workstations share SSH keys if the workstations are owned by different users. Inspected configuration of the Company's identity provider, version control system, and infrastructure to verify all users have MFA enabled. Inspected the configuration of the Company's identity and access management tool to verify that a password policy was applied to each user. Inspected configurations of AWS to verify that all employees/contractors have unique usernames. Additionally, verified that the root infrastructure account is not being used, all accounts are assigned to a group, and roles are assigned at the group level. Lastly, reviewed inactive accounts to verify that all inactive accounts that have not been disabled have been inactive for less than 90 days.	No exceptions noted.
The Company completes termination checklists to ensure that access is revoked for terminated employees and contractors within SLAs and that company equipment is returned as necessary.	Inspected logs from the infrastructure provider authorization system to verify employee and contractor access to infrastructure is removed within 24 business hours of authorization being rescinded. Inspected termination checklists to verify that terminated employee and contractor accounts were removed from critical systems within the specified SLA of the employee becoming unauthorized. Inspected the Company's Access Control Policy to verify it establishes a procedure for offboarding employees and contractors requiring deprovisioning of access to critical systems and the return of company property.	No exceptions noted.
Formal procedures are documented that outline the process the Company's staff follows to perform the following access control functions: - Adding new users - Modifying an existing user's access - Removing an existing user's access	Inspected the Company's security policies to verify that they require that employees may only access the customer data they need in order to complete their jobs. Inspected policy acknowledgements for all relevant employees to verify they had agreed to the Company's most recent version of its Access Control Policy. Inspected policy acknowledgements for all relevant employees to verify they had agreed to the Company's most recent version of its Information Security Roles and Responsibilities Policy.	No exceptions noted.

**SECTION IV - APPLICABLE TRUST SERVICES CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS
THROUGHOUT THE PERIOD JULY 16, 2024 TO JULY 15, 2025**

User access to system components is based on job role and function and requires a documented access request form and manager approval prior to access being provisioned.	Inspected policy acknowledgements for all relevant employees to verify they had agreed to the Company's most recent version of its Access Control Policy. Inspected a sample of access request tickets to verify user access follows the Company's Access Control Policy.	No exceptions noted. Per inquiry of management, there were no access request tickets within the examination period. As such, we were unable to test the Company's access request procedures.
Management conducts quarterly access reviews for the in-scope system components to help ensure that access is restricted appropriately. Tickets are created to remove or modify access as necessary in a timely manner.	Inspected logs from the infrastructure provider authorization system to verify employee/contractor access to infrastructure is restricted appropriately. Inspected a sample of access reviews to verify access to system components was reviewed by an appropriate member of management and in accordance with company policy.	No exceptions noted. Per inspection of the Company records, 2 of 4 access reviews were not conducted within the examination period.
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.		
Control	Control Test Performed by Auditor	Test Result(s)
The Company completes termination checklists to ensure that access is revoked for terminated employees and contractors within SLAs and that company equipment is returned as necessary.	Inspected logs from the infrastructure provider authorization system to verify employee and contractor access to infrastructure is removed within 24 business hours of authorization being rescinded. Inspected termination checklists to verify that terminated employee and contractor accounts were removed from critical systems within the specified SLA of the employee becoming unauthorized. Inspected the Company's Access Control Policy to verify it establishes a procedure for offboarding employees and contractors requiring deprovisioning of access to critical systems and the return of company property.	No exceptions noted.
User access to system components is based on job role and function and requires a documented access request form and manager approval prior to access being provisioned.	Inspected policy acknowledgements for all relevant employees to verify they had agreed to the Company's most recent version of its Access Control Policy. Inspected a sample of access request tickets to verify user access follows the Company's Access Control Policy.	No exceptions noted. Per inquiry of management, there were no access request tickets within the examination period. As such, we were unable to test the Company's access request procedures.
Management conducts quarterly access reviews for the in-scope system components to help ensure that access is restricted appropriately. Tickets are created to remove or modify access as necessary in a timely manner.	Inspected logs from the infrastructure provider authorization system to verify employee/contractor access to infrastructure is restricted appropriately. Inspected a sample of access reviews to verify access to system components was reviewed by an appropriate member of management and in accordance with company policy.	No exceptions noted. Per inspection of the Company records, 2 of 4 access reviews were not conducted within the examination period.

SECTION IV - APPLICABLE TRUST SERVICES CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS
THROUGHOUT THE PERIOD JULY 16, 2024 TO JULY 15, 2025

Formal procedures are documented that outline the process the Company's staff follows to perform the following access control functions: - Adding new users - Modifying an existing user's access - Removing an existing user's access	Inspected the Company's security policies to verify that they require that employees may only access the customer data they need in order to complete their jobs. Inspected policy acknowledgements for all relevant employees to verify they had agreed to the Company's most recent version of its Access Control Policy. Inspected policy acknowledgements for all relevant employees to verify they had agreed to the Company's most recent version of its Information Security Roles and Responsibilities Policy.	No exceptions noted.
CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.		
Control	Control Test Performed by Auditor	Test Result(s)
The Company completes termination checklists to ensure that access is revoked for terminated employees and contractors within SLAs and that company equipment is returned as necessary.	Inspected logs from the infrastructure provider authorization system to verify employee and contractor access to infrastructure is removed within 24 business hours of authorization being rescinded. Inspected termination checklists to verify that terminated employee and contractor accounts were removed from critical systems within the specified SLA of the employee becoming unauthorized. Inspected the Company's Access Control Policy to verify it establishes a procedure for offboarding employees and contractors requiring deprovisioning of access to critical systems and the return of company property.	No exceptions noted.
Criteria also addressed via subservice provider controls.		
CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.		
Control	Control Test Performed by Auditor	Test Result(s)
The Company's Asset Management Policy requires electronic media containing confidential information to be reformatted and/or destroyed in accordance with best practices prior to disposing of it.	Inspected policy acknowledgements for all relevant employees to verify they had agreed to the Company's most recent version of its Asset Management Policy.	No exceptions noted.
Customer data containing confidential information is purged or removed from the application environment, in accordance with best practices, when customers request deletion of data or upon leaving the service.	Inquired of management if customer data containing confidential information was purged or removed from the application environment. Inspected offboarding records to verify offboarding of former customer is complete.	Per inquiry of management, no customers requested data deletion during the examination period. Additionally, no customers left the service during the examination period. As such, we were unable to test the procedures for purging or removing customer data from the System.
Formal retention and disposal procedures are in place to guide the secure retention and disposal of company and customer data.	Inspected the Data Management Policy to verify that data retention and disposal procedures were documented to guide the secure retention and disposal of company and customer data.	No exceptions noted.

SECTION IV - APPLICABLE TRUST SERVICES CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS
THROUGHOUT THE PERIOD JULY 16, 2024 TO JULY 15, 2025

The Company maintains a formal inventory of production system assets. Assets are classified by type, owners, location, and type(s) of data accessed by the asset.	Inspected an inventory listing of information assets the Company maintains in order to protect inventory from security events to verify assets are labeled and categorized appropriately.	No exceptions noted.
Criteria also addressed via subservice provider controls.		
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.		
Control	Control Test Performed by Auditor	Test Result(s)
Firewalls are used and configured to prevent unauthorized access.	Inspected the configuration of the Company's laptops to verify that no two workstations share SSH keys if the workstations are owned by different users. Inspected the cloud provider configuration to verify all AWS EC2 instances have security groups configured to restrict inbound SSH (TCP port 22) traffic from the public internet (0.0.0.0/0). Inspected the configuration of AWS to verify that all EC2 instances have network ACLs or security groups attached. Inspected the configuration of AWS to verify that each RDS instance's attached Security Groups are only accessible by restricted IP addresses.	No exceptions noted.
Network and system hardening standards are documented, based on industry best practices, and reviewed by the Company at least annually.	Inspected the task tracker to verify that all tasks that are labeled with either 'account-create' or 'infra-change' tag were closed within the specified SLA. Inspected Company records to verify that terminated employees' accounts were removed from critical systems within the specified SLA of the employee becoming unauthorized. Inspected the cloud provider configuration to verify all AWS EC2 instances have security groups configured to restrict inbound SSH (TCP port 22) traffic from the public internet (0.0.0.0/0). Inspected the configuration of AWS to verify that all EC2 instances have network ACLs or security groups attached. Inspected the configuration of AWS to verify that all AWS Elastic Kubernetes Service (EKS) clusters have private endpoint access enabled for their control plane endpoints. Inspected the configuration of AWS to verify that AWS EKS clusters with public endpoint access enabled restrict access by setting specific CIDR blocks and do not allow traffic from all IP addresses (0.0.0.0/0 or ::0/0). Inspected the configuration of AWS to verify that all AWS EKS clusters have a cluster security group attached.	No exceptions noted.

SECTION IV - APPLICABLE TRUST SERVICES CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS
THROUGHOUT THE PERIOD JULY 16, 2024 TO JULY 15, 2025

Logging and monitoring tools are used to collect traffic and event logs from network devices, applications, and systems. Security alerts are generated, prioritized, and communicated to the designated responders for follow up. The Company uses these alerts to initiate, triage and, if necessary, remediate security issues based on their assigned priority.	Inspected the configuration for the tool that continuously monitors infrastructure packages and confirmed that it is active and alerts on vulnerabilities. Inspected the Company's records to verify that the Company is using a tool to monitor and evaluate security vulnerabilities in employee workstations. Inspected the configuration of AWS to verify that all linked accounts have CloudTrail enabled and at least one S3 bucket acting as a destination for server access logging or CloudTrail data event logging. Inspected the configuration of AWS to verify that GuardDuty is enabled on all accounts and regions. Inspected the configuration of AWS to verify that notifications have been configured for new GuardDuty threat detections on all accounts and regions. Inspected the configuration of AWS to verify that all VPCs have flow logs enabled and no S3 logging buckets grant access to the built-in AWS groups. Inspected the configuration of AWS to verify that all CloudWatch Log Groups are configured to retain logs for at least 365 days. Inspected the configuration of AWS to verify that all audit log types are enabled for your AWS EKS clusters.	No exceptions noted.
Secure data transmission protocols are used to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the admin page and log in of the Company's infrastructure provider to verify that all connections happen over SSL/TLS with a valid certificate from a reliable Certificate Authority. Inspected policy acknowledgements for all relevant employees to verify they had agreed to the Company's most recent version of its Cryptography Policy. Inspected the certificate used to encrypt all data in transit to verify it has not expired. Inspected the Company website configurations to verify (as specified on the business info page) redirects HTTP to HTTPS via a 3XX status code. Inspected the Company website configurations to verify it (as specified on the business info page) has a valid certificate and only accepts TLS connections using up-to-date cipher suites.	No exceptions noted.

SECTION IV - APPLICABLE TRUST SERVICES CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS
THROUGHOUT THE PERIOD JULY 16, 2024 TO JULY 15, 2025

Infrastructure supporting the service is patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure servers supporting the service are hardened against security threats.	Inspected the Company's task tracker to verify that all tasks that are labeled with a 'security' tag have a priority and owner assigned within the task tracker. Inspected alerts generated by the infrastructure-package vulnerability scanner to verify they're addressed within a specified SLA. Inspected the team's task tracker and confirmed security issues are tracked in a shared issue tracking system.	No exceptions noted.
Firewall rulesets are reviewed by the Company at least annually. Change tickets are created to track any firewall modifications as a result of the review.	Inspected the task tracker to verify that all tasks that are labeled with either 'account-create' or 'infra-change' tag were closed within the specified SLA. Inspected Company records to verify that terminated employees' accounts were removed from critical systems within the specified SLA of the employee becoming unauthorized. Inspected the cloud provider configuration to verify all AWS EC2 instances have security groups configured to restrict inbound SSH (TCP port 22) traffic from the public internet (0.0.0.0/0). Inspected the configuration of AWS to verify that all EC2 instances have network ACLs or security groups attached. Inspected the configuration of AWS to verify that all AWS Elastic Kubernetes Service (EKS) clusters have private endpoint access enabled for their control plane endpoints. Inspected the configuration of AWS to verify that AWS EKS clusters with public endpoint access enabled restrict access by setting specific CIDR blocks and do not allow traffic from all IP addresses (0.0.0.0/0 or ::0/0). Inspected the configuration of AWS to verify that all AWS EKS clusters have a cluster security group attached.	No exceptions noted.
Production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) token.	Inspected all user accounts with access to the infrastructure, the infrastructure root account, identity provider users, and the version control system to verify that each is configured with MFA.	No exceptions noted.
CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.		
Control	Control Test Performed by Auditor	Test Result(s)
The Company requires employee computers with access to the System to be encrypted.	Inspected the MDM tool to verify that the Company's employee computers are using full-disk encryption.	No exceptions noted.

SECTION IV - APPLICABLE TRUST SERVICES CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS
THROUGHOUT THE PERIOD JULY 16, 2024 TO JULY 15, 2025

Secure data transmission protocols are used to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the admin page and log in of the Company's infrastructure provider to verify that all connections happen over SSL/TLS with a valid certificate from a reliable Certificate Authority. Inspected policy acknowledgements for all relevant employees to verify they had agreed to the Company's most recent version of its Cryptography Policy. Inspected the certificate used to encrypt all data in transit to verify it has not expired. Inspected the Company website configurations to verify (as specified on the business info page) redirects HTTP to HTTPS via a 3XX status code. Inspected the Company website configurations to verify it (as specified on the business info page) has a valid certificate and only accepts TLS connections using up-to-date cipher suites.	No exceptions noted.
A mobile device management (the MDM) system is in place to centrally manage laptops supporting the service.	Inspected the MDM tool to verify that the Company tracks and monitors the status of employees' computers and service accounts using a tracking system. Inspected the MDM tool to verify that the Company's employee computers are running anti-malware software. Inspected the MDM tool to verify that the Company's employee computers are running a password manager. Inspected the MDM tool to verify that the Company's employee computers are using full-disk encryption. Inspected the MDM tool to verify that the Company's employee computers are using screen lock after a defined period of inactivity.	No exceptions noted.
CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.		
Control	Control Test Performed by Auditor	Test Result(s)
Anti-malware technology is deployed for environments commonly susceptible to malicious attack and is configured to be updated routinely, logged, and installed on all relevant systems.	Inspected the MDM tool to verify that the Company's employee computers are running anti-malware software.	No exceptions noted.
Infrastructure supporting the service is patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure servers supporting the service are hardened against security threats.	Inspected the Company's task tracker to verify that all tasks that are labeled with a 'security' tag have a priority and owner assigned within the task tracker. Inspected alerts generated by the infrastructure-package vulnerability scanner to verify they're addressed within a specified SLA. Inspected the team's task tracker and confirmed security issues are tracked in a shared issue tracking system.	No exceptions noted.

SECTION IV - APPLICABLE TRUST SERVICES CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS
THROUGHOUT THE PERIOD JULY 16, 2024 TO JULY 15, 2025

A formal systems development life cycle (SDLC) methodology is in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the Company's Secure Development Policy and Operations Security Policy to verify that it outlines considerations for planning, design, security, availability, implementation, and maintenance of changes.	No exceptions noted.
System Operations		
CC7.1 - To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.		
Control	Control Test Performed by Auditor	Test Result(s)
There are documented formal procedures that outline the process the Company's staff follows to perform the following functions related to IT/Engineering: - Vulnerability management - System monitoring	Inspected the Company's Operations Security Policy to verify that it is in place and outlines vulnerability management and system monitoring procedures. Inspected policy acknowledgements for all relevant employees to verify they had agreed to the Company's most recent version of its Operations Security Policy.	No exceptions noted.
Risk assessments are performed by the Company at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the Company's Risk Management Policy to verify there is a formal program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. Inspected the security risk assessment, which includes the risks, prioritization, and resulting action plans to verify it is documented in a risk register.	No exceptions noted.
The Company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected the configuration of the version control system and/or tickets in the task tracker to verify that production changes must be reviewed and approved by an independent technical resource prior to deployment to production. Inspected tickets from the version control system and task tracker to verify that production changes are tested, reviewed, and approved prior to being implemented in the production environment. Inspected tickets from the version control system and task tracker to verify that production changes are evaluated for their potential effect on the Company's security commitments.	No exceptions noted.
Vulnerability scans are performed continuously. A remediation plan is developed and changes are implemented to remediate all critical and high vulnerabilities, at a minimum, within a specified SLA.	Inspected the configuration for the tool that monitors infrastructure packages to verify that it is active and alerts on vulnerabilities. Inspected alerts generated by the infrastructure-package vulnerability scanner to verify they're addressed within a specified SLA. Inspected the Company's task tracker and confirmed security issues are tracked in a shared issue tracking system.	No exceptions noted.
Criteria also addressed via subservice provider controls.		

SECTION IV - APPLICABLE TRUST SERVICES CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS
THROUGHOUT THE PERIOD JULY 16, 2024 TO JULY 15, 2025

CC7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.		
Control	Control Test Performed by Auditor	Test Result(s)
Infrastructure monitoring tools are utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	Inspected the Company's infrastructure configuration to verify that the Company uses load balancers. Inspected the AWS configuration to verify that each AWS account in the Company has at least one Application Load Balancer (ALB) configured. Inspected the AWS configuration to verify that all AWS ALBs have AWS CloudWatch alarms configured to monitor their host health statuses and latency using specific AWS-provided metrics. Inspected the infrastructure monitoring configuration to verify that messaging queue age is monitored. Inspected the SQL database monitoring configuration to verify that memory, outstanding read/write requests, and disk I/O are monitored with configured alarm thresholds. Inspected the DynamoDB monitoring configuration to verify that all Amazon DynamoDB clusters enabled have CloudWatch alarms set for the FreeableMemory, VolumeReadIOPS, ReadIOPS, DiskQueueDepth, VolumeWriteIOPS and WriteIOPS metrics.	No exceptions noted.
A log management tool is utilized to identify trends that may have a potential impact on the Company's ability to achieve its security objectives.	Inspected the configuration of AWS to verify that all VPCs have flow logs enabled and no S3 logging buckets grant access to the built-in AWS groups. Inspected the configuration of AWS to verify that all linked accounts have CloudTrail enabled and at least one S3 bucket acting as a destination for server access logging or CloudTrail data event logging. Inspected the configuration of AWS to verify that all CloudWatch Log Groups are configured to retain logs for at least 365 days. Inspected the configuration of AWS to verify that all audit log types are enabled for your AWS EKS clusters.	No exceptions noted.
There are documented formal procedures that outline the process the Company's staff follows to perform the following functions related to IT/Engineering: - Vulnerability management - System monitoring	Inspected the Company's Operations Security Policy to verify that it is in place and outlines vulnerability management and system monitoring procedures. Inspected policy acknowledgements for all relevant employees to verify they had agreed to the Company's most recent version of its Operations Security Policy.	No exceptions noted.

SECTION IV - APPLICABLE TRUST SERVICES CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS
THROUGHOUT THE PERIOD JULY 16, 2024 TO JULY 15, 2025

Logging and monitoring tools are used to collect traffic and event logs from network devices, applications, and systems. Security alerts are generated, prioritized, and communicated to the designated responders for follow up. The Company uses these alerts to initiate, triage and, if necessary, remediate security issues based on their assigned priority.	Inspected the configuration for the tool that continuously monitors infrastructure packages and confirmed that it is active and alerts on vulnerabilities. Inspected the Company's records to verify that the Company is using a tool to monitor and evaluate security vulnerabilities in employee workstations. Inspected the configuration of AWS to verify that all linked accounts have CloudTrail enabled and at least one S3 bucket acting as a destination for server access logging or CloudTrail data event logging. Inspected the configuration of AWS to verify that GuardDuty is enabled on all accounts and regions. Inspected the configuration of AWS to verify that notifications have been configured for new GuardDuty threat detections on all accounts and regions. Inspected the configuration of AWS to verify that all VPCs have flow logs enabled and no S3 logging buckets grant access to the built-in AWS groups. Inspected the configuration of AWS to verify that all CloudWatch Log Groups are configured to retain logs for at least 365 days. Inspected the configuration of AWS to verify that all audit log types are enabled for your AWS EKS clusters.	No exceptions noted.
Vulnerability scans are performed continuously. A remediation plan is developed and changes are implemented to remediate all critical and high vulnerabilities, at a minimum, within a specified SLA.	Inspected the configuration for the tool that monitors infrastructure packages to verify that it is active and alerts on vulnerabilities. Inspected alerts generated by the infrastructure-package vulnerability scanner to verify they're addressed within a specified SLA.	No exceptions noted.
Infrastructure supporting the service is patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure servers supporting the service are hardened against security threats.	Inspected the Company's task tracker to verify that all tasks that are labeled with a 'security' tag have a priority and owner assigned within the task tracker. Inspected alerts generated by the infrastructure-package vulnerability scanner to verify they're addressed within a specified SLA. Inspected the team's task tracker and confirmed security issues are tracked in a shared issue tracking system.	No exceptions noted.
Penetration testing is performed at least annually. A remediation plan is developed and changes are implemented by the Company to remediate all critical and high vulnerabilities or findings at a minimum.	Inspected the report from the Company's latest penetration test to verify it was performed in the previous 12 months. Additionally, verified that all critical and high-priority findings were remediated as needed.	No exceptions noted.
Criteria also addressed via subservice provider controls.		

SECTION IV - APPLICABLE TRUST SERVICES CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS
THROUGHOUT THE PERIOD JULY 16, 2024 TO JULY 15, 2025

CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and if so, takes actions to prevent or address such failures.		
Control	Control Test Performed by Auditor	Test Result(s)
Security incidents, including instances of noncompliance, are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the Company's security incident response Policy and procedures.	Inquired of management to verify appropriate personnel are involved in reviewing the Incident Response Plan on at least an annual basis. Inspected the Incident Response Plan to verify that it included a section about tracking follow-ups and writing lessons learned after incidents. Inspected the Incident Response Plan to verify that it outlines formal procedure for responding to security events. Inspected the Company's procedure settings in its GRC tool to verify that an SLA for critical/high priority security bugs was set. Inquired of the Company about incidents that took place during the examination period that required the Incident Response Plan to be used to verify that the Incident Response Plan was followed. Inspected the Company's records to verify that the Incident Response Plan was executed for identified security incidents.	No exceptions noted.
Incident response policies and procedures are documented and communicated to authorized users.	Inspected policy acknowledgements for all relevant employees to verify they had agreed to the Company's most recent version of its Incident Response Plan. Inspected the Incident Response Plan to verify that it included a section about tracking follow-ups after incidents, writing lessons learned documents after incidents, outlines formal procedure for responding to security events, and names the individuals responsible for monitoring for and responding to incidents.	No exceptions noted.
Criteria also addressed via subservice provider controls.		
CC7.4 - The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.		
Control	Control Test Performed by Auditor	Test Result(s)
Infrastructure supporting the service is patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure servers supporting the service are hardened against security threats.	Inspected the Company's task tracker to verify that all tasks that are labeled with a `security` tag have a priority and owner assigned within the task tracker. Inspected alerts generated by the infrastructure-package vulnerability scanner to verify they're addressed within a specified SLA. Inspected the team's task tracker and confirmed security issues are tracked in a shared issue tracking system.	No exceptions noted.

SECTION IV - APPLICABLE TRUST SERVICES CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS
THROUGHOUT THE PERIOD JULY 16, 2024 TO JULY 15, 2025

Security incidents, including instances of noncompliance, are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the Company's security incident response Policy and procedures.	Inquired of management to verify appropriate personnel are involved in reviewing the Incident Response Plan on at least an annual basis. Inspected the Incident Response Plan to verify that it included a section about tracking follow-ups and writing lessons learned after incidents. Inspected the Incident Response Plan to verify that it outlines formal procedure for responding to security events. Inspected the Company's procedure settings in its GRC tool to verify that an SLA for critical/high priority security bugs was set. Inquired of the Company about incidents that took place during the examination period that required the Incident Response Plan to be used to verify that the Incident Response Plan was followed. Inspected the Company's records to verify that the Incident Response Plan was executed for identified security incidents.	No exceptions noted.
Incident response policies and procedures are documented and communicated to authorized users.	Inspected policy acknowledgements for all relevant employees to verify they had agreed to the Company's most recent version of its Incident Response Plan. Inspected the Incident Response Plan to verify that it included a section about tracking follow-ups after incidents, writing lessons learned documents after incidents, outlines formal procedure for responding to security events, and names the individuals responsible for monitoring for and responding to incidents.	No exceptions noted.
Vulnerability scans are performed continuously. A remediation plan is developed and changes are implemented to remediate all critical and high vulnerabilities, at a minimum, within a specified SLA.	Inspected the configuration for the tool that monitors infrastructure packages to verify that it is active and alerts on vulnerabilities. Inspected alerts generated by the infrastructure-package vulnerability scanner to verify they're addressed within a specified SLA. Inspected the Company's task tracker and confirmed security issues are tracked in a shared issue tracking system.	No exceptions noted.
Criteria also addressed via subservice provider controls.		
CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.		
Control	Control Test Performed by Auditor	Test Result(s)
Incident response policies and procedures are documented and communicated to authorized users.	Inspected policy acknowledgements for all relevant employees to verify they had agreed to the Company's most recent version of its Incident Response Plan. Inspected the Incident Response Plan to verify that it included a section about tracking follow-ups after incidents, writing lessons learned documents after incidents, outlines formal procedure for responding to security events, and names the individuals responsible for monitoring for and responding to incidents.	No exceptions noted.

SECTION IV - APPLICABLE TRUST SERVICES CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS
THROUGHOUT THE PERIOD JULY 16, 2024 TO JULY 15, 2025

The Company has a documented business continuity/disaster recovery (BC/DR) plan which is tested annually.	Inspected the Company's Business Continuity/Disaster Recovery (BC/DR) plan, to verify that it outlines a plan for testing key services to determine how they fare in a disaster scenario. Inspected evidence from the Company's latest disaster recovery test, which was performed in the prior 12 months.	No exceptions noted.
Security incidents, including instances of noncompliance, are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the Company's security incident response Policy and procedures.	Inquired of management to verify appropriate personnel are involved in reviewing the Incident Response Plan on at least an annual basis. Inspected the Incident Response Plan to verify that it included a section about tracking follow-ups and writing lessons learned after incidents. Inspected the Incident Response Plan to verify that it outlines formal procedure for responding to security events. Inspected the Company's procedure settings in its GRC tool to verify that an SLA for critical/high priority security bugs was set. Inquired of the Company about incidents that took place during the examination period that required the Incident Response Plan to be used to verify that the Incident Response Plan was followed. Inspected the Company's records to verify that the Incident Response Plan was executed for identified security incidents.	No exceptions noted.
The Incident Response Plan is tested by the Company on an annual basis.	Inquired of management to verify appropriate personnel are involved in reviewing the Incident Response Plan on at least an annual basis. Inspected the Incident Response Plan test documentation to verify the Incident Response Plan had been tested in the prior 12 months.	No exceptions noted.
Criteria also addressed via subservice provider controls.		
Change Management		
CC8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.		
Control	Control Test Performed by Auditor	Test Result(s)
Infrastructure supporting the service is patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure servers supporting the service are hardened against security threats.	Inspected the Company's task tracker to verify that all tasks that are labeled with a `security` tag have a priority and owner assigned within the task tracker. Inspected alerts generated by the infrastructure-package vulnerability scanner to verify they're addressed within a specified SLA. Inspected the team's task tracker and confirmed security issues are tracked in a shared issue tracking system.	No exceptions noted.

SECTION IV - APPLICABLE TRUST SERVICES CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS
THROUGHOUT THE PERIOD JULY 16, 2024 TO JULY 15, 2025

Access to migrate changes to production is restricted to authorized personnel.	Inspected the Company's version control system to verify that at least one approval is required to merge to the default branch for all production repositories. Inspected all user accounts with access to the version control system to verify that each is configured with MFA. Inspected the Company's version control system to verify that the visibility of all repositories has been set to private. Inspected the Company's version control system to verify that at least one production repository has been updated in the last 30 days. Inspected policy acknowledgements for all relevant employees to verify they had agreed to the Company's most recent version of its Operations Security Policy and Secure Development Policy.	No exceptions noted.
Network and system hardening standards are documented, based on industry best practices, and reviewed by the Company at least annually.	Inspected the task tracker to verify that all tasks that are labeled with either 'account-create' or 'infra-change' tag were closed within the specified SLA. Inspected Company records to verify that terminated employees' accounts were removed from critical systems within the specified SLA of the employee becoming unauthorized. Inspected the cloud provider configuration to verify all AWS EC2 instances have security groups configured to restrict inbound SSH (TCP port 22) traffic from the public internet (0.0.0.0/0). Inspected the configuration of AWS to verify that all EC2 instances have network ACLs or security groups attached. Inspected the configuration of AWS to verify that all AWS Elastic Kubernetes Service (EKS) clusters have private endpoint access enabled for their control plane endpoints. Inspected the configuration of AWS to verify that AWS EKS clusters with public endpoint access enabled restrict access by setting specific CIDR blocks and do not allow traffic from all IP addresses (0.0.0.0/0 or ::0/0). Inspected the configuration of AWS to verify that all AWS EKS clusters have a cluster security group attached.	No exceptions noted.
A formal systems development life cycle (SDLC) methodology is in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the Company's Secure Development Policy and Operations Security Policy to verify that it outlines considerations for planning, design, security, availability, implementation, and maintenance of changes.	No exceptions noted.

SECTION IV - APPLICABLE TRUST SERVICES CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS
THROUGHOUT THE PERIOD JULY 16, 2024 TO JULY 15, 2025

The Company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected the configuration of the version control system and/or tickets in the task tracker to verify that production changes must be reviewed and approved by an independent technical resource prior to deployment to production. Inspected tickets from the version control system and task tracker to verify that production changes are tested, reviewed, and approved prior to being implemented in the production environment. Inspected tickets from the version control system and task tracker to verify that production changes are evaluated for their potential effect on the Company's security commitments.	No exceptions noted.
Vulnerability scans are performed continuously. A remediation plan is developed and changes are implemented to remediate all critical and high vulnerabilities, at a minimum, within a specified SLA.	Inspected the configuration for the tool that monitors infrastructure packages to verify that it is active and alerts on vulnerabilities. Inspected alerts generated by the infrastructure-package vulnerability scanner to verify they're addressed within a specified SLA. Inspected the Company's task tracker and confirmed security issues are tracked in a shared issue tracking system.	No exceptions noted.
Penetration testing is performed at least annually. A remediation plan is developed and changes are implemented by the Company to remediate all critical and high vulnerabilities or findings at a minimum.	Inspected the report from the Company's latest penetration test to verify it was performed in the previous 12 months. Additionally, verified that all critical and high-priority findings were remediated as needed.	No exceptions noted.
Risk Mitigation		
CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.		
Control	Control Test Performed by Auditor	Test Result(s)
Business Continuity and Disaster Recovery plans are in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.	Inspected the Company's Business Continuity Plan to verify it defines an operational and organizational strategy in the event of a disruption and has been updated in the past year. Inspected the Company's Disaster Recovery Plan to verify that it outlines steps to take in the event of a disaster and has been updated in the past year.	No exceptions noted.
Cybersecurity insurance is maintained to mitigate the financial impact of business disruptions.	Inspected the Company's cybersecurity insurance policy to verify the coverage is adequate and was maintained throughout the period.	No exceptions noted.
Risk assessments are performed by the Company at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the Company's Risk Management Policy to verify there is a formal program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. Inspected the security risk assessment, which includes the risks, prioritization, and resulting action plans to verify it is documented in a risk register.	No exceptions noted.

SECTION IV - APPLICABLE TRUST SERVICES CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS
THROUGHOUT THE PERIOD JULY 16, 2024 TO JULY 15, 2025

The Company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the Company's Risk Management Policy to verify there is a formal program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC9.2 - The entity assesses and manages risks associated with vendors and business partners.		
Control	Control Test Performed by Auditor	Test Result(s)
A vendor management program is in place. Components of this program include: - Maintaining a list of critical third-party vendors. - Monitoring and reviewing service delivery. - Requirements for third-party vendors to maintain their own security practices and procedures. - Annually reviewing critical third-party attestation reports or performing a vendor risk assessment.	Inspected the Company's Third-Party Management Policy to verify that the Company provides a process for documenting and managing vendor relationships through maintaining a list of vendors, requirements for third-party vendors to maintain their own security practices and procedures, and annually reviewing critical third-party attestation reports or performing a vendor risk assessment.	No exceptions noted.
The Company has written agreements in place with vendors and related third-parties.	Inspected the vendor list to verify that the Company maintains a complete list of vendors. Inspected a sample of executed vendor agreements to verify executed agreements are in place between the Company and its vendors.	No exceptions noted.

The background is a solid blue color. In the top-left corner, there are overlapping geometric shapes in light blue and green. In the bottom-right corner, there are similar overlapping geometric shapes in green and light blue.

**SECTION V:
OTHER INFORMATION PROVIDED BY MXHERO, INC.**

Management's Response to Audit Findings

Control	Control Test	Test Result	Management's Response
Management conducts quarterly access reviews for the in-scope system components to help ensure that access is restricted appropriately. Tickets are created to remove or modify access as necessary in a timely manner.	Inspected a sample of access reviews to verify access to system components was reviewed by an appropriate member of management and in accordance with company policy.	Per inspection of the Company records, 2 of 4 access reviews were not conducted within the examination period.	During the examination period, only two of the four quarterly access reviews were formally documented. This was due to a timing inconsistency between the documented quarterly cadence and the Company's operational reality. mxHero has maintained a highly stable workforce with no new hires or contractor onboarding during the period and minimal access changes over several years. Access provisioning and deprovisioning continued to require documented management approval, MFA remained enforced, dormant accounts were automatically disabled, and no unauthorized access or security incidents were identified. Management has determined that a bi-annual documented review more appropriately aligns with the Company's low turnover environment and existing continuous monitoring controls. Accordingly, the Access Control Policy is being updated to reflect a bi-annual review cadence going forward.