



**System and Organization Controls (SOC) 2 Type 2 Report**  
**Patchworks Media Ltd's Description of Its Patchworks Platform**  
**Relevant to Security, Availability, and Confidentiality**  
**Throughout the Period February 1, 2025 to July 31, 2025**

## Table of Contents

**Section 1: Independent Service Auditor's Report**

**Section 2: Assertion of Patchworks Media Ltd Management**

**Section 3: Patchworks' Description of Its Patchworks Platform Throughout the Period February 1, 2025 to July 31, 2025**

**Section 4: Trust Services Criteria, Related Controls and Tests of Controls Relevant to the Security, Confidentiality, and Availability Categories**

**Section 5: Other Information Provided by Patchworks That Is Not Covered by the Service Auditor's Report**

## Section 1: Independent Service Auditor's Report

To: Patchworks Media Ltd ("Patchworks" or "the Company")

### Scope

We have examined Patchworks' accompanying description of its Patchworks Platform found in Section 3 titled "Patchworks' Description of Its Patchworks Platform Throughout the Period February 1, 2025 to July 31, 2025" (description), based on the criteria for a description of a service organization's system set forth in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria)*, (*description criteria*) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period February 1, 2025 to July 31, 2025, to provide reasonable assurance that Patchworks' service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability and Confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

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

Patchworks uses a subservice organization for infrastructure and data hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Patchworks, to achieve Patchworks' service commitments and system requirements based on the applicable trust services criteria. The description presents Patchworks' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Patchworks' 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 information included in Section 5, "Other Information Provided by Patchworks That Is Not Covered by the Service Auditor's Report", is presented by Patchworks' management to provide additional information and is not part of Patchworks' description of its Patchworks Platform made available to user entities throughout the period February 1, 2025 to July 31, 2025. Information included in Patchworks' responses to testing exceptions has not been subjected to the procedures applied in the examination and, accordingly, we express no opinion on it.

### Service Organization's Responsibilities

Patchworks 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 Patchworks' service commitments and system requirements were achieved. In Section 2, Patchworks has provided the accompanying assertion titled "Assertion of Patchworks Media Ltd Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Patchworks is also 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 operating 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 opinion.

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

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves 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.

## 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 report 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 or 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 we tested and the nature, timing, and results of those tests are listed in Section 4, "Trust Services Criteria, Related Controls and Tests of Controls Relevant to the Security, Confidentiality, and Availability Categories" of this report.

## Controls That Were Not Tested During the Period

The Company's description of its system discusses the following controls implemented and operated during the period February 1, 2025 to July 31, 2025 that were not tested as part of our procedures:

- REQ-50: All incidents related to security are logged, tracked, evaluated, and communicated to affected parties by management until the Company has recovered from the incidents.
- REQ-67: Customer data is purged from the application environment upon customer request.

During the period February 1, 2025 to July 31, 2025, the Company did not experience the above control activities that would warrant the operation of the controls during the period.

Because the controls described above were not required to operate during the period, we did not test the operating effectiveness of those controls as evaluated using the following trust services criteria (TSC):

- TSC 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.
- TSC C1.2: The entity disposes of confidential information to meet the entity's objectives related to confidentiality.

## Opinion

In our opinion, in all material respects—

- a. The description presents the Patchworks Platform that was designed and implemented throughout the period February 1, 2025 to July 31, 2025, in accordance with the description criteria.
- b. The controls stated in the description were suitably designed throughout the period February 1, 2025 to July 31, 2025, to provide reasonable assurance that Patchworks' service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Patchworks' controls throughout that period.
- c. The controls stated in the description operated effectively throughout the period February 1, 2025 to July 31, 2025, to provide reasonable assurance that Patchworks' 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 Patchworks' controls operated effectively throughout that period.

## Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Patchworks, user entities of the Patchworks Platform during some or all of the period February 1, 2025 to July 31, 2025, business partners of Patchworks subject to risks arising from interactions with the Patchworks Platform, 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, business partners, 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.

*Laika Compliance LLC*

Arlington, Virginia

August 21, 2025

## Section 2: Assertion of Patchworks Media Ltd Management

We have prepared the accompanying description in Section 3 titled "Patchworks' Description of Its Patchworks Platform Throughout the Period February 1, 2025 to July 31, 2025" (description), based on the criteria for a description of a service organization's system set forth in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria) (description criteria)*. The description is intended to provide report users with information about the Patchworks Platform that may be useful when assessing the risks arising from interactions with Patchworks' system, particularly information about system controls that Patchworks has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability and Confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

Patchworks uses a subservice organization for infrastructure and data hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Patchworks, to achieve Patchworks' service commitments and system requirements based on the applicable trust services criteria. The description presents Patchworks' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Patchworks' controls. The description does not disclose the actual controls at the subservice organization.

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

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

- a. The description presents the Patchworks Platform that was designed and implemented throughout the period February 1, 2025 to July 31, 2025, in accordance with the description criteria.
- b. The controls stated in the description were suitably designed throughout the period February 1, 2025 to July 31, 2025, to provide reasonable assurance that Patchworks' service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Patchworks' controls throughout that period.
- c. The controls stated in the description operated effectively throughout the period February 1, 2025 to July 31, 2025, to provide reasonable assurance that Patchworks' 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 Patchworks' controls operated effectively throughout that period.

Our description of the Patchworks Platform discusses the following controls implemented during the period February 1, 2025 to July 31, 2025 that were not required to operate due to non occurrence of the activities:

- REQ-50: All incidents related to security are logged, tracked, evaluated, and communicated to affected parties by management until the Company has recovered from the incidents.
- REQ-67: Customer data is purged from the application environment upon customer request.

During the period February 1, 2025 to July 31, 2025, Patchworks did not experience the above control activities that would warrant the operation of the controls during the period.

Patchworks Media Ltd

## Section 3: Patchworks' Description of Its Patchworks Platform Throughout the Period February 1, 2025 to July 31, 2025

### Overview of Operations

Patchworks Media Ltd (“Patchworks” or “the Company”) offers the Patchworks Platform, an Integration Platform as a Service (IPaaS) for retail and e-commerce businesses. The Patchworks Platform allows businesses to connect their core business applications to key ecommerce systems allowing retailers to simplify technology stack integration. The Patchworks Platform also eliminates the need for manual data entry by automating the flow of data across the business.

The system description in this section of the report details the Patchworks Platform. Any other Company services are not within the scope of this report. The accompanying description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at any subservice organizations (see below for further discussion of the subservice organization).

### Principal Service Commitments and System Requirements

Service commitments are declarations made by management to customers regarding the performance of the Patchworks Platform. The Terms of Service and Service Level Objectives include the communication of the Company's commitments to its customers.

System requirements are specifications regarding how the Patchworks Platform should function to meet the Company's principal commitments to customers. System requirements are specified in the Company's policies and procedures, system design documentation, contracts with customers, and in government regulations.

The Company's principal service commitments and system requirements related to the Patchworks Platform include the following:

Trust Services Category	Service Commitments	System Requirements
<p><b>Security</b></p>	<p>Patchworks will use commercially reasonable efforts to prevent any unauthorized use, access, processing, destruction, loss or disclosure of any customer materials stored or processed by the Patchworks Platform.</p>	<ul style="list-style-type: none"> <li>• Change Management</li> <li>• Encryption Standards</li> <li>• Identity and Access Management</li> <li>• Security Awareness Training</li> <li>• Security Incident Response</li> <li>• Security Monitoring and Reporting</li> <li>• Threat and Vulnerability Management</li> <li>• Vendor Risk Management</li> </ul>

Trust Services Category	Service Commitments	System Requirements
<p><b>Confidentiality</b></p>	<p>Patchworks will: (i) not use any customer confidential information except as necessary to exercise its rights or perform its obligations under the Terms of Service or as expressly authorized in writing; (ii) use the same degree of care to protect customer confidential information as it uses to protect its own confidential information of like nature; and (iii) not disclose customer confidential information to any person or entity except those with a need to know and who have entered into written confidentiality agreements.</p>	<ul style="list-style-type: none"> <li>• Data Classification</li> <li>• Data Retention and Disposal</li> <li>• Information Sharing and Confidentiality Standards</li> </ul>
<p><b>Availability</b></p>	<p>Patchworks will guarantee a 99.5% uptime for the Patchworks Platform exclusive of service outages attributed to (i) scheduled maintenance of which customers have notice; (ii) failures by customers, customer third party providers, suppliers or any factors beyond Patchworks reasonable control; and (iii) internet connectivity issues (customers cannot connect to the internet).</p>	<ul style="list-style-type: none"> <li>• Business Continuity and Disaster Recovery</li> <li>• Data Backup, Recovery, and Replication</li> </ul>

**The Components of the System Used to Provide the Service**

The boundaries of the Patchworks Platform are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the Patchworks Platform.

The components that directly support the services provided to customers are described in the subsections below.

**INFRASTRUCTURE**

The Company utilizes Amazon Web Services (AWS) to provide the resources to host the Patchworks Platform. The Company leverages the experience and resources of AWS to scale quickly and securely as necessary to meet current and future demand. However, the Company is responsible for designing and configuring the architecture within AWS to ensure security and resiliency requirements are met.

The in-scope hosted infrastructure also consists of multiple supporting tools, as shown in the table below:

Infrastructure		
Production Tool	Business Function	Hosted Location
Amazon Elastic Compute Cloud (EC2)	Cloud Compute	AWS
Amazon Elastic Kubernetes Service (EKS)	Container Orchestration	AWS
Amazon Relational Database Service (RDS)	Data Storage	AWS
Amazon Simple Storage Service (S3)	Data Storage	AWS
AWS Key Management System (KMS)	Cryptographic Key Management	AWS
AWS Security Groups	Network Traffic Control	AWS

**SOFTWARE**

Software consists of the programs and software that support the Patchworks Platform. The list of software and ancillary software used to build, support, secure, maintain, and monitor the Patchworks Platform includes the following applications, as shown in the table below:

Software	
Production Application	Business Function
Amazon Elastic Container Registry (ECR)	Container Registry
Cloudflare	Network Security and Traffic Management
GitHub	Code Repository
GitHub Actions	Continuous Integration and Delivery
Google Workspace	Single Sign-On (SSO) and Authentication
Grafana	Infrastructure Monitoring
Jira	Ticketing System

Software	
Production Application	Business Function
Slack	Alert Communication
Snyk	Code Scanning
Terraform	Configuration Management
Wazuh	Threat Detection, Log Management and Anti-Malware

**PEOPLE**

The Company develops, manages, and secures the Patchworks Platform via separate departments. The responsibilities of these departments involved in the governance, management, operation, security, and use of the Patchworks Platform are defined in the following table:

People	
Group/Role Name	Function
Customer Success	Responsible for managing and strengthening customer relationships to drive adoption, satisfaction, and retention of products and services.
Engineering	Responsible for the design, development, testing, deployment, and maintenance of software and system components.
Executive Management	Responsible for providing strategic leadership, overseeing company-wide activities, and ensuring organizational goals and objectives are established, communicated, and achieved.
Human Resources	Responsible for managing the employee lifecycle, including recruitment, onboarding, role definition, performance management, and terminations, while ensuring compliance with employment laws and policies.
Marketing	Responsible for developing and executing marketing strategies to enhance brand awareness and generate leads.

People	
Group/Role Name	Function
Product	Responsible for defining product vision, strategy, and roadmap, gathering customer requirements, and coordinating with stakeholders to deliver features that meet market and business needs.
Sales	Responsible for revenue generation, client acquisition, and management of the sales pipeline.

**PROCEDURES**

Procedures include the automated and manual procedures involved in the operation of the Patchworks Platform. Procedures are developed and documented by the respective teams for a variety of processes. These procedures are drafted in alignment with the overall Information Security Policy and are updated and approved as necessary for changes in the business, but no less than annually.

The following table details the procedures as they relate to the operation of the Patchworks Platform:

Procedure	Description
Logical Access	How the Company restricts logical access, provides and removes that access, and prevents unauthorized access.
System Operations	How the Company manages the operation of the system and detects and mitigates processing deviations, including logical and physical security deviations.
Configuration and Change Management	How the Company identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
Risk and Compliance	How the Company identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.
Data Backup and Storage	How the Company manages data backups to allow for data restorations to occur if needed.
Business Continuity and Disaster Recovery (BC/DR)	How the Company identifies the steps to be taken in the event of a disaster to help resume business operations.

Procedure	Description
Data Classification and Handling	How the Company classifies data included in the service and the procedures for handling the data.
Incident Response Plan	How the Company identifies the steps to be taken in the event of a security incident.

**DATA**

Data refers to transaction streams, files, data stores, tables, and other outputs used or processed by the Patchworks Platform. Through the application programming interface (API), the customer or end-user defines and controls the data they load into and store in the Patchworks Platform production network. Once stored in the environment, the data is accessed remotely from customer systems via the Internet.

Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established in customer contracts.

The Company has deployed secure methods and protocols for transmission of confidential and sensitive information over public networks. Data stores housing customer data are encrypted at rest.

**SYSTEM INCIDENTS**

A system event is defined as an occurrence that could lead to the loss of, or disruption to, operations, services, or functions and result in Patchworks' failure to achieve its service commitments or system requirements. Such an occurrence may arise from actual or attempted access or use by internal or external parties and (a) impair (or potentially impair) the availability, integrity, or confidentiality of information or systems; (b) result in unauthorized disclosure or theft of information or other assets or the destruction of corruption of data; or (c) cause damage to systems. Such occurrences also may arise from the failure of the Patchworks Platform to process data as designed or from the loss, corruption, or destruction of data used by the Patchworks Platform.

On the other hand, a system incident is defined as a system event that requires action on the part of Patchworks management to prevent or reduce the impact of the event on Patchworks' achievement of its service commitments and system requirements.

There were no identified significant system incidents that (a) were the result of controls that were not suitably designed or operating effectively to achieve one or more of the service commitments and system requirements or (b) otherwise resulted in a significant failure in the achievement of one or more of those service commitments and system requirements from February 1, 2025 to July 31, 2025.

**The Applicable Trust Services Criteria and Related Controls**

**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 availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.
- **Confidentiality:** Information designated as confidential is protected to meet the entity's objectives.

- **Availability:** Information and systems are available for operation and use to meet the entity's objectives.

Many of the criteria used to evaluate a system are shared amongst all the trust services categories; for example, the criteria related to risk assessment apply to the Security, Confidentiality, and Availability categories. As a result, the trust services criteria for the Security, Confidentiality, and Availability categories are organized into (a) the criteria that are common to all the trust services categories (common criteria) and (b) additional specific criteria applicable only to a single category. The common criteria are suitable for evaluating the effectiveness of controls to achieve the entity's system objectives related to the security category; no additional control activity criteria are needed. For the categories of Confidentiality and Availability, a complete set of criteria consists of (a) the common criteria and (b) the control activity criteria applicable to each specific trust services category being reported on. The criteria for each trust services category being reported on are considered complete only if all the criteria associated with that category are addressed.

The common criteria are organized as follows:

1. **Control environment:** The criteria relevant to how the entity is structured and the processes the entity has implemented to manage and support people within its operating units. This includes criteria addressing accountability, integrity, ethical values, qualifications of personnel, and the environment in which they function.
2. **Information and communication:** The criteria relevant to how the entity 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 the entity (i) identifies potential risks that would affect the entity'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 the entity 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 the entity restricts logical and physical access, provides and removes that access, and prevents unauthorized access.
7. **System operations:** The criteria relevant to how the entity manages the operation of a system and detects and mitigates processing deviations, including logical and physical security deviations.
8. **Change management:** The criteria relevant to how the entity 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 the entity identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

This report is focused solely on the Security, Confidentiality, and Availability categories.

## CONTROL ENVIRONMENT

### INTEGRITY AND ETHICAL VALUES

Patchworks places emphasis on ethics and communication within the organization. Management communicates and oversees the implementation of the Code of Conduct to new and current employees and contractors. The Code of Conduct describes employee and contractor responsibilities and expected behavior regarding data and information system usage. Employees and contractors receive the Code of Conduct upon hire and sign an acknowledgment to confirm that they have received, read, and understand its contents.

Patchworks commits to the highest level of integrity in dealing with its customers, vendors, and workforce. This commitment to integrity is promulgated with established policies that cover a variety of business and integrity objectives.

As part of the compliance effort, Patchworks maintains a complete inventory list of all third parties. Such third parties are contractually required to maintain relevant elements of information security policy requirements, and to report cybersecurity incidents, in a timely manner.

### **OVERSIGHT AND AUTHORITY**

The Risk Committee is tasked with governance, oversight, and responsibilities relative to internal control. The Risk Committee includes members that are independent of the internal control function. The Risk Committee meets quarterly and maintains formal meeting minutes.

### **ORGANIZATIONAL STRUCTURE**

Patchworks' organizational structure provides a framework for planning, executing, and controlling business operations. The organizational structure assigns roles and responsibilities to provide for adequate staffing, efficiency of operations, and the segregation of duties. Roles and responsibilities are formally documented and include responsibilities for the oversight and implementation of the security and control environment. Management has also established authority and appropriate lines of reporting for key personnel. Patchworks follows a structured onboarding process to assist new employees as they become familiar with processes, systems, policies, and procedures. Patchworks places emphasis on ethics and communication within the organization.

### **MANAGEMENT'S PHILOSOPHY AND OPERATING STYLE**

Patchworks' senior management takes a hands-on approach to running the business. Senior management is heavily involved in all phases of the business operations. The senior management team remains in close contact with all personnel and consistently emphasizes appropriate behavior to all personnel and key vendor personnel.

### **AUTHORITY AND RESPONSIBILITY**

Management and employees are assigned appropriate levels of authority and responsibility to facilitate effective internal control.

### **HUMAN RESOURCES**

Upon hire and annually thereafter, all personnel must successfully complete training courses covering basic information security practices that support the functioning of an effective risk management program. The training courses are designed to assist employees in identifying and responding to cybersecurity threats, including social engineering, phishing, pharming, and avoiding inappropriate security practices.

If an employee is found to be violating company policies, additional training is provided, or other disciplinary actions are taken.

Employees with job responsibilities that fall directly within the incident response program have additional requirements to complete technical and job-specific training throughout the year. Additionally, those employees who have direct access to customer and employee data will receive specific training around incident management, information handling, and data protection.

When onboarding new personnel, reference checks are performed by Patchworks management.

### **INFORMATION AND COMMUNICATION**

Patchworks has an Information Security Policy to ensure that employees understand their individual roles and responsibilities concerning processes, as well as controls to ensure that significant events are communicated in a timely manner. The policy includes formal and informal training programs and the use of email, instant messaging, and other mechanisms to communicate time-sensitive information and processes for security and system availability purposes that notify key personnel when issues are identified. The Information Security Policy helps users understand how their roles and responsibilities relate to the system and the

policy is communicated to all users.

Patchworks has also published documentation that describes the security features of the service, internal security-related processes and controls, and conformity to regulatory requirements.

## RISK ASSESSMENT AND MITIGATION

Patchworks has performed a risk assessment during the design and implementation of the control objectives and related controls described in this report. As part of the risk assessment, Patchworks identified the threats and vulnerabilities relevant to the security of Patchworks business operations and rated the risk posed by each identified vulnerability. This rating allowed for the design and implementation of controls to mitigate the most significant risks to the security of Patchworks' service.

The risk assessment is performed annually, at a minimum, or in response to any major updates to the product, client base, or business plan.

When conducting the risk assessment, Patchworks first identified threats and vulnerabilities relevant to the security of business operations. For each identified vulnerability, Patchworks considered:

- The likelihood of impact (i.e., the likelihood of the vulnerability being exploited), and
- The severity of impact (i.e., how damaging an exploitation of the vulnerability would be).

The likelihood and severity of impact estimations were then used to establish a risk ranking for each vulnerability.

## MONITORING

The systems within the boundary are configured to prevent and detect vulnerabilities. In addition to prompt reviews of system alerts, management provides monitoring and audit logging in the form of preventive, detective, and corrective reporting. Relevant output from monitoring and detection mechanisms is distributed to executive and management personnel. Security testing, both automated and manual, occurs at regular intervals. Code dependency vulnerability scans are performed on an ongoing basis to identify, quantify, and prioritize vulnerabilities. Penetration testing is performed annually to identify vulnerabilities that could be exploited to gain access to the production environment. Vulnerabilities identified are ranked by the security team and management and remediated based on the Company's vulnerability management policies and procedures.

Anti-malware technology is deployed for environments commonly susceptible to malicious attacks and is configured to be updated routinely, logged, and installed on production servers.

The Company utilizes a distributed approach in order to scale the security monitoring function by using a combination of commercially available tools, custom code, and an instant messaging platform. The Company has created a system that provides for the determination of attributions for the most critical security-relevant events and target notifications are sent to the staff with the authority and the context necessary to vet that security alert. The interface of this system allows the targeted staff member to either resolve the security alert if they can do so safely or to escalate to the appropriate team if a response is required.

## CONTROL ACTIVITIES

**Information Security:** An Information Security Policy has been documented and implemented to provide policies and procedures governing the protection of confidential and sensitive information. The Information Security Policy is communicated and distributed to authorized users. In the event of a significant change to the Information Security Policy, a communication is sent to all authorized users regarding the changes.

The Information Security Policy is reviewed and updated on an annual basis. The Information Security Policy defines information security responsibilities for all personnel. Where security responsibilities apply, roles are related to the policy and procedures that define their activity within their associated responsibilities. Security awareness training is provided to all employees upon hire and

on an annual basis thereafter to ensure that personnel understand their security roles and responsibilities.

Patchworks also communicates security roles and responsibilities to vendors and other third parties. Marketing and contractual materials that describe the services and scope of work provided to clients are documented and maintained to ensure that employees, contractors, vendors, and clients understand their roles and responsibilities.

## LOGICAL ACCESS

An Access Control Policy is documented and includes guidance for provisioning and deprovisioning users; access reviews and recertification; and restricting access based on separation of duties and least privilege. Periodic access reviews are conducted to help ensure that system access is restricted appropriately and access is modified or removed where necessary. In addition, password configuration settings for system components are managed in compliance with Patchworks' Password Policy.

Access to system components is based on job role, function, and requires a documented access request with manager approval prior to access being provisioned. Users must also be assigned unique user IDs before being allowed access to system components. Access rights and privileges are granted to user IDs based on the principle of least privilege and Role-Based Access Control (RBAC) protocols. User access is limited to that which is required for the performance of job duties. Privileged access to system components is restricted to authorized users with a business need and access to production infrastructure is restricted to authorized users with valid multi-factor authentication (MFA) tokens. Access to system components is revoked within stipulated timelines as part of the termination process.

## SYSTEM OPERATIONS

An Incident Response Policy has been documented and implemented to guide preparation, detection, response, analysis and repair, communication, follow-up, and training for any class of security breach or incident. The responsibilities in the event of a breach, the steps of a breach, and the importance of information security are defined for all employees. The Incident Response Team employs industry-standard diagnosis procedures (such as incident identification, registration and verification, as well as initial incident classification and prioritizing actions) to drive resolution during business-impacting events.

Patchworks reviews, triages, and communicates all incident alerts to the Incident Response Team to initiate the incident response process. Post-mortems are convened after any significant operational issue, regardless of external impact. Documentation of the investigation is conducted to determine that the root cause is captured and that preventative actions may be taken for the future.

## CHANGE MANAGEMENT

A Change Management Policy has been documented and implemented to guide the processes of change request, documentation, review, evaluation, approval, scheduling, testing, and implementation. Changes that may affect system availability and system security are communicated to management and any partners who may be affected.

System configuration standards are documented and implemented to ensure that all systems and network devices are properly and securely configured. Hardening standards are documented and include guidance on baseline security requirements for production systems before deployment to the production environment.

Secure Software Development: Patchworks applies a systematic approach to software development so that changes to customer-impacting services are reviewed, tested, approved, and communicated. Prior to deployment to production environments, changes are:

- Developed in a development environment that is segregated from the production environment.
- Reviewed by peers for technical aspects and appropriateness.
- Tested to confirm the changes will behave as expected when applied and not adversely impact performance.
- Approved by authorized team members to provide appropriate oversight and understanding of business impact.

## AVAILABILITY

System capacity is evaluated continuously to help ensure that processing capacity can meet demand. The risks that would prevent Patchworks from meeting its availability commitments and requirements are diverse. Availability includes the consideration of risks during normal business operations and during routine failure of elements of the system, as well as risks related to the continuity of business operations during a natural or man-made disaster.

The Company has designed its controls to address the following availability risks:

- Insufficient processing capacity.
- Insufficient internet response time.
- Loss of processing capability due to a power outage.
- Loss of communication with user entities due to a break in telecommunication services.
- Loss of key processing equipment, facilities, or personnel due to a natural disaster.

Availability risks are addressed through the use and testing of various monitoring tools and backup and disaster recovery plans and procedures. The Patchworks Platform's production data is backed up on a regular basis to support data availability and recovery. Data backup restoration tests are performed periodically to verify data recoverability.

A business continuity and disaster recovery (BC/DR) plan is documented to support continuity and recovery of critical services and business processes after unexpected business interruptions. The BC/DR plan is tested periodically to assess the effectiveness of management's readiness to respond to unexpected business interruptions.

In evaluating the suitability of the design of availability controls, Patchworks considers the likely causes of data loss, the commitments and requirements related to availability, the timeliness of backup procedures, the reliability of the backup process, and the ability to restore backed-up data. In evaluating the design of data availability controls, Patchworks considers that most data loss does not result from disasters, but from routine processing errors and failures of system elements.

## CONFIDENTIALITY

The confidentiality category refers to the protection of customer information as committed by the Company's service level agreements. The confidentiality of the Patchworks Platform is dependent on many aspects of the Company's operations. The risks that would prevent the Company from meeting its confidentiality commitments and requirements are diverse. The Company has designed its controls to address both internal and external confidentiality risks specifically related to protection from improper use and disclosure (including the monitoring of vendor services), as well as the proper retention and disposal of confidential customer information.

Confidentiality risks are addressed through policies and procedures covering the use, retention, and disposal of confidential data, data classification policies and procedures, confidentiality and information sharing agreements, remote access and transmission restrictions, and vendor risk assessments.

In evaluating the suitability of the design and operating effectiveness of confidentiality controls, the Company considers the likely causes of improper disclosure or handling of confidential information and the commitments and requirements related to confidentiality.

## COMPLEMENTARY USER ENTITY CONTROLS (CUECs)

The Company's controls related to the Patchworks Platform cover only a portion of overall internal control for each user entity of the Patchworks Platform. It is not feasible for the service commitments, system requirements, and applicable criteria related to the system to be achieved solely by the Company. Therefore, each user entity's internal control should be evaluated in conjunction with the Company's controls and the related tests and results described in Section 4 of this report, taking into account the related

CUECs identified for the specific criterion. In order for user entities to rely on the controls reported herein, each user entity must evaluate its own internal control environment to determine whether the identified CUECs have been implemented and are operating effectively.

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

Criteria	Complementary User Entity Controls (CUECs)
CC2.1	<ul style="list-style-type: none"> <li>• User entities have policies and procedures to report any material changes to their overall control environment that may adversely affect services being performed by the Company according to contractually specified time frames.</li> <li>• Controls to provide reasonable assurance that the Company is notified of changes in:                             <ul style="list-style-type: none"> <li>◦ User entity vendor security requirements.</li> <li>◦ The authorized user list.</li> </ul> </li> </ul>
CC2.3	<ul style="list-style-type: none"> <li>• It is the responsibility of the user entity to have policies and procedures to:                             <ul style="list-style-type: none"> <li>◦ Inform their employees and users that their information or data is being used and stored by the Company.</li> <li>◦ Determine how to file inquiries, complaints, and disputes to be passed on to the Company.</li> </ul> </li> </ul>
CC6.1	<ul style="list-style-type: none"> <li>• User entities grant access to the Company's system to authorized and trained personnel.</li> <li>• User entities deploy physical security and environmental controls for all devices and access points residing at their operational facilities, including remote employees or at-home agents for which the user entity allows connectivity.</li> </ul>
CC6.6	<ul style="list-style-type: none"> <li>• Controls to provide reasonable assurance that policies and procedures are deployed over user IDs and passwords that are used to access services provided by the Company.</li> </ul>
CC7.4	<ul style="list-style-type: none"> <li>• User entities are responsible for notifying the Company of any security incidents that are discovered.</li> </ul>

**SUBSERVICE ORGANIZATION AND COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS (CSOCs)**

The Company uses AWS as a subservice organization for infrastructure and data hosting services. The Company's controls related to the Patchworks Platform cover only a portion of the overall internal control for each user entity of the Patchworks Platform. The description does not extend to the infrastructure and data hosting services provided by the subservice organization. Section 4 of this report and the description of the system only cover the Trust Services Criteria and related controls of the Company and exclude the related controls of AWS.

Although the subservice organization has been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organization. Accordingly, CSOCs are expected to be in place at AWS, as described in the CSOC table below.

The Company management receives and reviews the AWS SOC 2 report annually. In addition, through its operational activities, Company management monitors the services performed by AWS to determine whether operations and controls expected to be implemented are functioning effectively. Management also communicates with the subservice organization to monitor compliance

with the service agreement, stay informed of changes planned at the hosting facility, and relay any issues or concerns to AWS management.

It is not feasible for the service commitments, system requirements, and applicable criteria related to the Patchworks Platform to be achieved solely by the Company. Therefore, each user entity's internal control must be evaluated in conjunction with the Company's controls and related tests and results described in Section 4 of this report, taking into account the related CSOCs expected to be implemented at AWS as described below.

Criteria	Complementary Subservice Organization Controls (CSOCs)
CC6.1	<ul style="list-style-type: none"> <li>• AWS is responsible for encrypting customer data at rest and in transit within the managed infrastructure to mitigate the risk of unauthorized access to sensitive data.</li> <li>• AWS is responsible for implementing access control over the managed infrastructure to mitigate the risk of unauthorized access or privilege escalation.</li> </ul>
CC6.4	<ul style="list-style-type: none"> <li>• AWS is responsible for restricting physical access to its data centers to authorized personnel to mitigate the risk of physical intrusion or unauthorized access to systems.</li> <li>• AWS is responsible for monitoring its data centers 24/7 using closed-circuit cameras and on-site security personnel to mitigate the risk of undetected unauthorized access or physical tampering.</li> </ul>
CC6.5	<ul style="list-style-type: none"> <li>• AWS is responsible for securely decommissioning and physically destroying production assets in its control to mitigate the risk of data recovery from retired equipment.</li> </ul>
CC6.6	<ul style="list-style-type: none"> <li>• AWS is responsible for applying security patches to the managed infrastructure as part of routine maintenance to mitigate the risk of vulnerabilities being exploited due to outdated systems.</li> </ul>
CC7.2 A1.2	<ul style="list-style-type: none"> <li>• AWS is responsible for installing fire suppression and detection systems and monitoring environmental conditions at its data centers to mitigate the risk of data center outages due to fire, temperature fluctuations, or environmental hazards.</li> <li>• AWS is responsible for protecting its data centers against power disruptions using uninterruptible power supply (UPS) systems to mitigate the risk of unexpected service outages and data loss.</li> <li>• AWS is responsible for the ongoing maintenance of environmental protection systems at its data centers to mitigate the risk of equipment failure or system downtime due to degraded infrastructure.</li> </ul>
CC8.1	<ul style="list-style-type: none"> <li>• AWS is responsible for implementing managed infrastructure changes to mitigate the risk of unauthorized or untested changes affecting system availability, integrity, or confidentiality.</li> </ul>

**SPECIFIC CRITERIA NOT RELEVANT TO THE SYSTEM**

There were no specific Security, Availability and Confidentiality Trust Services Criteria as set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria) that were not relevant to the system as presented in this report.

### **SIGNIFICANT CHANGES TO THE SYSTEM**

There were no changes that are likely to affect report users' understanding of how the Patchworks Platform was used to provide the service from February 1, 2025 to July 31, 2025.

### **REPORT USE**

The description does not omit or distort information relevant to the Patchworks Platform 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 their particular needs.

## Section 4: Trust Services Criteria, Related Controls and Tests of Controls Relevant to the Security, Confidentiality, and Availability Categories

This SOC 2 Type 2 Report was prepared in accordance with the AICPA Attestation Standards based on the criteria for a description of a service organization's system set forth in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria)*, (*description criteria*) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period February 1, 2025 to July 31, 2025.

### Description of Testing Procedures Performed

Laika Compliance LLC evaluated the design and operating effectiveness of the controls listed in this section throughout the period February 1, 2025 to July 31, 2025. Our evaluation included procedures we considered necessary in the circumstances to determine whether the control activities were suitably designed and operating to achieve the service commitments and system requirements based on the relevant trust services criteria throughout the period February 1, 2025 to July 31, 2025.

In determining the nature, timing, and extent of procedures performed, we considered the following factors:

- The nature and timing of the controls being tested.
- The types of evidential matter.
- The appropriateness of the control design and operation relative to the applicable trust services criteria.
- The assessed level of control risk.
- The entity's control environment and related governance processes.

The procedures performed included:

- **Inquiry:** Conducted detailed interviews with relevant stakeholders to obtain evidence that the control operated during the period. This procedure was accompanied by additional testing, as noted below, to corroborate the information obtained through inquiry.
- **Observation:** Observed the performance of the control during the period to obtain evidence of the application of the specific control activity.
- **Inspection:** Inspected relevant documentation, configurations, and reports to obtain evidence that the control activity was designed and operating as intended.
- **Reperformance:** Obtained the documentation used in the performance of the control activity and independently reperfomed the control or process to verify its accuracy and operation.

### Reliability of Information Produced by Patchworks

For tests of controls requiring the use of information produced by the entity (IPE) (e.g., controls requiring system-generated populations for sample-based testing), a combination of the following

procedures were performed, where possible, based on the nature of the IPE to address the completeness, accuracy, and data integrity of the data or reports used:

- Inspected the source of the IPE.
- Inspected the query, script, or parameters used to generate the IPE.
- Tied data between the IPE and the source.
- Inspected the IPE for anomalous gaps in sequence or timing to determine the data was complete, accurate, and maintained its integrity.

Furthermore, in addition to the above procedures, for tests of controls requiring management’s use of IPE in the execution of controls (e.g., periodic reviews of user access privileges); an inspection of management’s procedures, as applicable, to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or reports was performed. While these procedures were not specifically called out in the test procedures listed in this section, they were completed as a component of our testing to support the evaluation of whether or not the information was sufficiently precise and detailed for purposes of fully testing the controls identified by Patchworks.

This section of the report includes 2 tables:

Table 1: Patchworks Controls Mapped to the Security, Confidentiality, and Availability Criteria

Table 2: Description of Tests of Controls, Service Auditor Tests, and Results of Tests

**Table 1: Patchworks Controls Mapped to the Security, Confidentiality, and Availability Criteria**

CC1.0 - Control Environment		
Criteria	Applicable Control Activities	Criteria Description
CC1.1	REQ-7 REQ-8 REQ-9 REQ-10 REQ-11 REQ-14	The entity demonstrates a commitment to integrity and ethical values.
CC1.2	REQ-3 REQ-4	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

CC1.0 - Control Environment		
Criteria	Applicable Control Activities	Criteria Description
CC1.3	REQ-2 REQ-4 REQ-15 REQ-16	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
CC1.4	REQ-12 REQ-13 REQ-14 REQ-15	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
CC1.5	REQ-7 REQ-8 REQ-14 REQ-15	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

CC2.0 - Information and Communication		
Criteria	Applicable Control Activities	Criteria Description
CC2.1	REQ-4 REQ-19 REQ-20 REQ-39 REQ-46 REQ-47	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.
CC2.2	REQ-2 REQ-12 REQ-13 REQ-15 REQ-56	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

<b>CC2.0 - Information and Communication</b>		
<b>Criteria</b>	<b>Applicable Control Activities</b>	<b>Criteria Description</b>
CC2.3	REQ-5 REQ-6 REQ-22	The entity communicates with external parties regarding matters affecting the functioning of internal control.

<b>CC3.0 - Risk Assessment</b>		
<b>Criteria</b>	<b>Applicable Control Activities</b>	<b>Criteria Description</b>
CC3.1	REQ-17 REQ-18	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
CC3.2	REQ-17 REQ-19 REQ-58 REQ-59	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.
CC3.3	REQ-17 REQ-19	The entity considers the potential for fraud in assessing risks to the achievement of objectives.
CC3.4	REQ-17 REQ-19 REQ-44 REQ-45 REQ-52	The entity identifies and assesses changes that could significantly impact the system of internal control.

<b>CC4.0 - Monitoring Activities</b>		
<b>Criteria</b>	<b>Applicable Control Activities</b>	<b>Criteria Description</b>
CC4.1	REQ-4 REQ-19 REQ-20 REQ-23 REQ-44 REQ-45 REQ-46 REQ-47	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
CC4.2	REQ-4 REQ-19 REQ-20 REQ-23	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.

<b>CC5.0 - Control Activities</b>		
<b>Criteria</b>	<b>Applicable Control Activities</b>	<b>Criteria Description</b>
CC5.1	REQ-17 REQ-20	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
CC5.2	REQ-17 REQ-20	The entity also selects and develops general control activities over technology to support the achievement of objectives.

CC5.0 - Control Activities		
Criteria	Applicable Control Activities	Criteria Description
CC5.3	REQ-1 REQ-17 REQ-21 REQ-24 REQ-32 REQ-42 REQ-48 REQ-51 REQ-53 REQ-60 REQ-65	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

CC6.0 - Logical and Physical Access		
Criteria	Applicable Control Activities	Criteria Description
CC6.1	REQ-25 REQ-26 REQ-28 REQ-33 REQ-34 REQ-36 REQ-54 REQ-57	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.
CC6.2	REQ-29 REQ-30 REQ-31	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.

CC6.0 - Logical and Physical Access		
Criteria	Applicable Control Activities	Criteria Description
CC6.3	REQ-29 REQ-30 REQ-31	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.
CC6.4	<b>The Company's production environment is hosted at third-party data centers, which are carved out for purposes of this report.</b>	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.
CC6.5	REQ-32 REQ-33	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.
CC6.6	REQ-27 REQ-35 REQ-37 REQ-40 REQ-43	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
CC6.7	REQ-35 REQ-39	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.
CC6.8	REQ-38 REQ-39 REQ-43	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.

CC7.0 - System Operations		
Criteria	Applicable Control Activities	Criteria Description
CC7.1	REQ-19 REQ-46 REQ-47 REQ-52	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.

CC7.0 - System Operations		
Criteria	Applicable Control Activities	Criteria Description
CC7.2	REQ-39 REQ-40 REQ-41 REQ-43 REQ-44 REQ-45 REQ-46 REQ-47	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.
CC7.3	REQ-39 REQ-44 REQ-45 REQ-46 REQ-47 REQ-48	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.
CC7.4	REQ-43 REQ-48 REQ-49 REQ-50	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.
CC7.5	REQ-48 REQ-49 REQ-58 REQ-59	The entity identifies, develops, and implements activities to recover from identified security incidents.

CC8.0 - Change Management		
Criteria	Applicable Control Activities	Criteria Description
CC8.1	REQ-43 REQ-54 REQ-55 REQ-57	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

CC9.0 - Risk Mitigation		
Criteria	Applicable Control Activities	Criteria Description
CC9.1	REQ-17 REQ-48 REQ-49 REQ-58 REQ-59 REQ-63	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.
CC9.2	REQ-22 REQ-23	The entity assesses and manages risks associated with vendors and business partners.

A1.0 - Additional Criteria for Availability		
Criteria	Applicable Control Activities	Criteria Description
A1.1	REQ-41 REQ-64	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.
A1.2	REQ-58 REQ-59 REQ-60 REQ-62 REQ-63	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.

<b>A1.0 - Additional Criteria for Availability</b>		
<b>Criteria</b>	<b>Applicable Control Activities</b>	<b>Criteria Description</b>
A1.3	REQ-58 REQ-59 REQ-60 REQ-61	The entity tests recovery plan procedures supporting system recovery to meet its objectives.

<b>C1.0 - Additional Criteria for Confidentiality</b>		
<b>Criteria</b>	<b>Applicable Control Activities</b>	<b>Criteria Description</b>
C1.1	REQ-22 REQ-32 REQ-65 REQ-66	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.
C1.2	REQ-67	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.

**Table 2: Description of Tests of Controls, Service Auditor Tests, and Results of Tests**

Control activities and test procedures performed in connection with determining the design and operating effectiveness of controls relative to the applicable Trust Services Criteria are described below.

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-1	An Information Security Policy is documented and defines the information security rules and requirements for the service environment. The policy is version controlled, reviewed annually, approved by management, and communicated to authorized users.	Inspected the Information Security Policy and policy repository to determine that an Information Security Policy was documented, defined the information security rules and requirements for the service environment, was version controlled, reviewed annually, approved by management, and communicated to authorized users.	<b>No exceptions noted.</b>
REQ-2	Management has established defined roles and responsibilities to oversee the implementation of the security and control environment.	Inspected the Information Security Policy to determine that management had established defined roles and responsibilities to oversee the implementation of the security and control environment.	<b>No exceptions noted.</b>
REQ-3	The Risk Committee is tasked with governance, oversight, and responsibilities relative to internal control. The Risk Committee includes members that are independent of the internal control function.	Inspected the Risk Committee charter to determine that the Risk Committee was tasked with governance, oversight, and responsibilities relative to internal control and the Risk Committee included members that were independent of the internal control function.	<b>No exceptions noted.</b>
REQ-4	The Risk Committee meets quarterly and maintains formal meeting minutes.	Inspected the Risk Committee meeting minutes for a sample of quarters to determine that the Risk Committee met quarterly and maintained formal meeting minutes.	<b>No exceptions noted.</b>
REQ-5	The Terms of Service and Service Level Objectives include the communication of the Company's commitments to its customers.	Inspected the Terms of Service and Service Level Objectives to determine that the Company's commitments were communicated to customers.	<b>No exceptions noted.</b>
REQ-6	Technical support resources related to system operations are provided on the Company's website.	Inspected the Company's website to determine that technical support resources related to system operations were provided on the Company's website.	<b>No exceptions noted.</b>

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-7	The Code of Conduct describes employee and contractor responsibilities and expected behavior regarding data and information system usage.	Inspected the Code of Conduct to determine that it described employee and contractor responsibilities and expected behavior regarding data and information system usage.	<b>No exceptions noted.</b>
REQ-8	Upon hire, employees and contractors acknowledge that they have read and agree to the Code of Conduct.	Inspected the Code of Conduct acknowledgments for a sample of new employees and contractors to determine that new employees and contractors received and acknowledged that they had read and agreed to the Code of Conduct upon hire.	<b>No exceptions noted.</b>
REQ-9	The employee and contractor confidentiality agreement prohibits any disclosure of information and other data to which the employee or contractor has been granted access.	Inspected the employee and contractor confidentiality agreement to determine that it prohibited the disclosure of information and other data to which the employee or contractor had been granted access.	<b>No exceptions noted.</b>
REQ-10	Upon hire, employees and contractors acknowledge that they have read and agree to the confidentiality agreement.	Inspected the confidentiality agreement acknowledgments for a sample of new employees and contractors to determine that new employees and contractors received and acknowledged that they had read and agreed to the confidentiality agreement upon hire.	<b>No exceptions noted.</b>
REQ-11	New employees and contractors offered employment and are subject to reference checks prior to their start date.	Inspected the reference check results for a sample of new employees and contractors to determine that new employees and contractors were subject to reference checks prior to their start date.	<b>No exceptions noted.</b>
REQ-12	New employees and contractors complete security awareness training upon hire.	Inspected the training records for a sample of new employees and contractors to determine that new employees and contractors completed security awareness training upon hire.	<b>No exceptions noted.</b>

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-13	Employees and contractors complete security awareness training annually.	Inspected the training records for a sample of employees and contractors to determine that employees completed security awareness training annually.	<b>Exceptions noted. For 1 of 8 sampled employees and contractors, an annual security awareness training was not completed.</b>
REQ-14	Managers complete performance appraisals for direct reports annually.	Inspected the performance appraisals for a sample of employees and contractors to determine that managers completed performance appraisals for direct reports annually.	<b>Exceptions noted. For 1 of 8 sampled employees and contractors, an annual performance appraisal was not completed.</b>
REQ-15	Job descriptions are documented for employees and contractors supporting the service and include authorities and responsibilities in support of the system.	Inspected the job descriptions for a sample of employees and contractors supporting the service to determine that job descriptions were documented and included authorities and responsibilities in support of the system.	<b>No exceptions noted.</b>
REQ-16	An organization chart is documented and defines the organizational structure and reporting lines.	Inspected the organization chart to determine that an organization chart was documented and defined the organizational structure and reporting lines.	<b>No exceptions noted.</b>
REQ-17	A Risk Management Policy is documented and 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 Risk Management Policy to determine that a Risk Management Policy was documented and included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	<b>No exceptions noted.</b>
REQ-18	The Company specifies its objectives in its annual risk assessment to enable the identification and assessment of risks related to the objectives.	Inspected the risk assessment results to determine that the Company specified its objectives in its annual risk assessment to enable the identification and assessment of risks related to the objectives.	<b>No exceptions noted.</b>

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-19	A risk assessment is performed annually. As part of this process, threats and changes 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 risk assessment results to determine that a risk assessment was performed annually and, as part of this process, threats and changes to service commitments were identified, risks were formally assessed, and the risk assessment included a consideration of the potential for fraud and how fraud may have impacted the achievement of objectives.	<b>No exceptions noted.</b>
REQ-20	As part of its annual risk assessment, management selects and develops manual and IT general control activities that contribute to the mitigation of identified risks.	Inspected the risk assessment results to determine that as part of its annual risk assessment, management selected and developed manual and IT general control activities that contributed to the mitigation of identified risks.	<b>No exceptions noted.</b>
REQ-21	A Vendor Management Policy is documented and includes guidance on performing the following vendor management functions: - Requirements for the classification of third-party vendors - Requirements for the assessment of risks resulting from the procurement of third-party services - Annually reviewing critical third-party attestation reports or performing a vendor risk assessment	Inspected the Vendor Management Policy to determine that a Vendor Management Policy was documented and included guidance on performing the following vendor management functions: - Requirements for the classification of third-party vendors - Requirements for the assessment of risks resulting from the procurement of third-party services - Annually reviewing critical third-party attestation reports or performing a vendor risk assessment	<b>No exceptions noted.</b>
REQ-22	Formal agreements are in place with critical vendors. These agreements include commitments applicable to that entity.	Inspected the contracts for a sample of critical vendors to determine that formal agreements were in place with critical vendors and the agreements included commitments applicable to that entity.	<b>No exceptions noted.</b>

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-23	<p>A third-party attestation report is reviewed annually for all critical vendors. Exceptions noted in the reports are evaluated to determine their impact on the service.</p>	<p>Inspected the third-party attestation report review results for a sample of critical vendors to determine that a third-party attestation report was reviewed annually for all critical vendors and exceptions noted in the reports were evaluated to determine their impact on the service.</p>	<p><b>No exceptions noted.</b></p>
REQ-24	<p>An Access Control Policy is documented and includes guidance for performing the following system access control functions:</p> <ul style="list-style-type: none"> <li>- Provisioning users</li> <li>- Deprovisioning users</li> <li>- Access reviews and recertification</li> <li>- Restricting access based on separation of duties and least privilege</li> </ul>	<p>Inspected the Access Control Policy to determine that an Access Control Policy was documented and included guidance for performing the following system access control functions:</p> <ul style="list-style-type: none"> <li>- Provisioning users</li> <li>- Deprovisioning users</li> <li>- Access reviews and recertification</li> <li>- Restricting access based on separation of duties and least privilege</li> </ul>	<p><b>No exceptions noted.</b></p>
REQ-25	<p>Authentication to the following system components requires unique usernames and passwords:</p> <ul style="list-style-type: none"> <li>- Network</li> <li>- Patchworks Platform</li> <li>- Operating System (OS)</li> <li>- Data Stores</li> <li>- AWS Console</li> <li>- Code Repository</li> </ul>	<p>Inspected the system configurations and observed login attempts to determine that authentication to the following system components required unique usernames and passwords:</p> <ul style="list-style-type: none"> <li>- Network</li> <li>- Patchworks Platform</li> <li>- OS</li> <li>- Data Stores</li> <li>- AWS Console</li> <li>- Code Repository</li> </ul>	<p><b>No exceptions noted.</b></p>

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-26	Passwords for the following system components are configured according to the Password Policy: <ul style="list-style-type: none"> <li>- Network</li> <li>- Patchworks Platform</li> <li>- OS</li> <li>- Data Stores</li> <li>- AWS Console</li> <li>- Code Repository</li> </ul>	Inspected the Password Policy and compared to password configurations for the following system components to determine that passwords were configured according to the Password Policy: <ul style="list-style-type: none"> <li>- Network</li> <li>- Patchworks Platform</li> <li>- OS</li> <li>- Data Stores</li> <li>- AWS Console</li> <li>- Code Repository</li> </ul>	No exceptions noted.
REQ-27	Access to production infrastructure is restricted to authorized users with valid multi-factor authentication (MFA) tokens.	Inspected the MFA configurations to determine that access to production infrastructure was restricted to authorized users with valid MFA tokens.	No exceptions noted.
REQ-28	Privileged access to the following system components is restricted to authorized users with a business need: <ul style="list-style-type: none"> <li>- Network</li> <li>- Patchworks Platform</li> <li>- OS</li> <li>- Data Stores</li> <li>- AWS Console</li> <li>- Code Repository</li> </ul>	Inspected the system access listings, inquired of management, and compared each user's access privileges to their job role to determine that privileged access to the following system components was restricted to authorized users with a business need: <ul style="list-style-type: none"> <li>- Network</li> <li>- Patchworks Platform</li> <li>- OS</li> <li>- Data Stores</li> <li>- AWS Console</li> <li>- Code Repository</li> </ul>	No exceptions noted.

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
<p><b>REQ-29</b></p>	<p>Semi-annual access reviews are conducted to help ensure that system access is restricted appropriately for the following system components:</p> <ul style="list-style-type: none"> <li>- Network</li> <li>- Patchworks Platform</li> <li>- OS</li> <li>- Data Stores</li> <li>- AWS Console</li> <li>- Code Repository</li> </ul> <p>The reviews are documented, and access is modified or removed where applicable.</p>	<p>Inspected the access review results for a sample of semi-annual periods to determine that semi-annual access reviews were conducted to help ensure that system access was restricted appropriately, the reviews were documented, and access was modified or removed where applicable for the following system components:</p> <ul style="list-style-type: none"> <li>- Network</li> <li>- Patchworks Platform</li> <li>- OS</li> <li>- Data Stores</li> <li>- AWS Console</li> <li>- Code Repository</li> </ul>	<p><b>No exceptions noted.</b></p>
<p><b>REQ-30</b></p>	<p>Access to system components is based on job role, function, and requires a documented access request with manager approval prior to access being provisioned.</p>	<p>Inspected the access request tickets for a sample of users that received access to system components to determine that access to system components was based on job role, function, and required a documented access request with manager approval prior to access being provisioned.</p>	<p><b>No exceptions noted.</b></p>
<p><b>REQ-31</b></p>	<p>Access to system components is revoked within 24 hours of termination as part of the termination process.</p>	<p>Inspected the termination tickets for a sample of terminated users to determine that access to system components was revoked within 24 hours of termination as part of the termination process.</p> <p>Inspected the listing of terminated users and compared against the privileged access system listings to determine that terminated users did not retain access to the system components after their separation.</p>	<p><b>No exceptions noted.</b></p> <p><b>No exceptions noted.</b></p>
<p><b>REQ-32</b></p>	<p>A Data Retention and Disposal Policy is documented and includes guidance for the secure retention and disposal of customer data.</p>	<p>Inspected the Data Retention and Disposal Policy to determine that a Data Retention and Disposal Policy was documented and included guidance for the secure retention and disposal of customer data.</p>	<p><b>No exceptions noted.</b></p>

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-33	An inventory of production system assets is maintained by management.	Inspected the production system asset inventory to determine that an inventory of production system assets was maintained by management.	<b>No exceptions noted.</b>
REQ-34	Encryption is enabled for data stores housing customer data.	Inspected the encryption configurations to determine that encryption was enabled for data stores housing customer data.	<b>No exceptions noted.</b>
REQ-35	Secure data transmission protocols are used to encrypt customer data when transmitted over public networks.	Inspected the transmission protocol configurations to determine that secure data transmission protocols were used to encrypt customer data when transmitted over public networks.	<b>No exceptions noted.</b>
REQ-36	The network is segmented to prevent unauthorized access to customer data.	Inspected the network configurations to determine that the network was segmented to prevent unauthorized access to customer data.	<b>No exceptions noted.</b>
REQ-37	AWS security groups are configured to prevent unauthorized access to the production environment.	Inspected the AWS security group configurations to determine that AWS security groups were configured to prevent unauthorized access to the production environment.	<b>No exceptions noted.</b>
REQ-38	Anti-malware technology is deployed for environments commonly susceptible to malicious attacks and is configured to be updated routinely, logged, and installed on production servers.	Inspected the anti-malware software configurations to determine that anti-malware technology was deployed for environments commonly susceptible to malicious attacks and was configured to be updated routinely, logged, and installed on production servers.	<b>No exceptions noted.</b>

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-39	A log management tool is utilized to monitor and identify security events and trends that may have a potential impact on the Company's ability to achieve its security objectives and generates alerts when security events occur.	Inspected the log management tool dashboard, configurations, and an example alert notification to determine that a log management tool was utilized to monitor and identify security events and trends that may have had a potential impact on the Company's ability to achieve its security objectives and generated alerts when security events occurred.	<b>No exceptions noted.</b>
REQ-40	An intrusion detection system (IDS) is used to provide continuous monitoring of the Company's network and early detection and prevention of potential security breaches and generates alerts when security events occur.	Inspected the IDS dashboard and alerting configurations to determine that an IDS was used to provide continuous monitoring of the Company's network and early detection and prevention of potential security breaches and generated alerts when security events occurred.	<b>No exceptions noted.</b>
REQ-41	A system monitoring tool is utilized to monitor system availability and performance and generates alerts when specific, predefined thresholds are met.	Inspected the system monitoring tool dashboard, configurations, and an example alert notification to determine that a system monitoring tool was utilized to monitor system availability and performance and generated alerts when specific, predefined thresholds were met.	<b>No exceptions noted.</b>
REQ-42	A Vulnerability Management Policy is documented and includes guidance for performing the following vulnerability management functions: <ul style="list-style-type: none"> <li>- Methods for identifying vulnerabilities and frequency</li> <li>- Assessing the severity of identified vulnerabilities</li> <li>- Prioritizing and implementing remediation or mitigation activities for identified vulnerabilities based on severity and defined timelines</li> </ul>	Inspected the Vulnerability Management Policy to determine that a Vulnerability Management Policy was documented and included guidance for performing the following vulnerability management functions: <ul style="list-style-type: none"> <li>- Methods for identifying vulnerabilities and frequency</li> <li>- Assessing the severity of identified vulnerabilities</li> <li>- Prioritizing and implementing remediation or mitigation activities for identified vulnerabilities based on severity and defined timelines</li> </ul>	<b>No exceptions noted.</b>

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-43	Infrastructure supporting the service is patched as a part of routine maintenance to help ensure that systems supporting the service are hardened against security threats.	Inspected the infrastructure configurations to determine that infrastructure supporting the service was patched as a part of routine maintenance to help ensure that systems supporting the service were hardened against security threats.	<b>No exceptions noted.</b>
REQ-44	Penetration testing is performed annually to identify vulnerabilities that could be exploited to gain access to the production environment.	Inspected the penetration test results to determine that penetration testing was performed annually to identify vulnerabilities that could have been exploited to gain access to the production environment.	<b>No exceptions noted.</b>
REQ-45	A remediation plan is developed and changes are implemented to remediate all critical and high vulnerabilities identified during the annual penetration test.	Inspected the remediation tickets for the critical and high vulnerabilities identified during the penetration test to determine that a remediation plan was developed and changes were implemented to remediate all critical and high vulnerabilities identified during the annual penetration test.	<b>No exceptions noted.</b>
REQ-46	Code dependency vulnerability scans are performed on an ongoing basis to identify, quantify, and prioritize vulnerabilities.	Inspected the vulnerability scan configurations and scan results to determine that code dependency vulnerability scans were performed on an ongoing basis to identify, quantify, and prioritize vulnerabilities.	<b>No exceptions noted.</b>
REQ-47	A remediation plan is developed and changes are implemented to remediate all critical and high vulnerabilities identified during ongoing code dependency vulnerability scans.	Inspected the remediation tickets for the critical and high vulnerabilities identified during the code dependency vulnerability scans to determine that a remediation plan was developed and changes were implemented to remediate all critical and high vulnerabilities identified during ongoing code dependency vulnerability scans.	<b>No exceptions noted.</b>
REQ-48	An Incident Response Policy is documented and includes guidance for detecting, responding to, and recovering from security events and incidents.	Inspected the Incident Response Policy to determine that an Incident Response Policy was documented and included guidance for detecting, responding to, and recovering from security events and incidents.	<b>No exceptions noted.</b>

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-49	The incident response plan is tested annually to assess the effectiveness of the incident response program.	Inspected the incident response plan test results to determine that the incident response plan was tested annually to assess the effectiveness of the incident response program.	<b>No exceptions noted.</b>
REQ-50	All incidents related to security are logged, tracked, evaluated, and communicated to affected parties by management until the Company has recovered from the incidents.	Inquired of management and inspected the security incident repository to determine that the circumstances that warrant the operation of the control did not occur during the period.	<b>Not tested. No security incidents occurred during the period. As a result, no operating effectiveness testing could be performed to determine whether all incidents related to security were logged, tracked, evaluated, and communicated to affected parties by management until the Company had recovered from the incidents.</b>
REQ-51	Hardening standards are documented and include guidance on baseline security requirements for production systems before deployment to the production environment.	Inspected the hardening standards to determine that hardening standards were documented and included guidance on baseline security requirements for production systems before deployment to the production environment.	<b>No exceptions noted.</b>
REQ-52	A configuration management tool (CMT) is used to ensure that system configurations are deployed consistently throughout the environment.	Inspected the CMT configurations to determine that a CMT was used to ensure that system configurations were deployed consistently throughout the environment.	<b>No exceptions noted.</b>
REQ-53	A Change Management Policy is documented and includes guidance for documenting, testing, reviewing, and approving changes to information systems.	Inspected the Change Management Policy to determine that a Change Management Policy was documented and included guidance for documenting, testing, reviewing, and approving changes to information systems.	<b>No exceptions noted.</b>

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-54	Access to migrate changes to production is restricted to authorized personnel.	Inspected the system access listings, inquired of management, and compared each user's access privileges to their job role to determine that access to migrate changes to production was restricted to authorized personnel.	<b>No exceptions noted.</b>
REQ-55	Changes to software and infrastructure components are authorized, documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected the change request tickets for a sample of software and infrastructure changes to determine that changes to software and infrastructure components were authorized, documented, tested, reviewed, and approved prior to being implemented in the production environment.	<b>Exceptions noted. For 2 of 20 sampled changes, evidence was not maintained to demonstrate that the changes were approved prior to being implemented in the production environment.</b>
REQ-56	System changes are communicated to authorized internal users.	Inspected the change request tickets for a sample of system changes to determine that system changes were communicated to authorized internal users.	<b>No exceptions noted.</b>
REQ-57	Branch protection rules are configured in the development tool to help ensure code quality, prevent accidental or malicious changes, enforce security and compliance requirements, and maintain the stability of critical branches.	Inspected the branch protection rule configurations to determine that branch protection rules were configured in the development tool to help ensure code quality, prevent accidental or malicious changes, enforce security and compliance requirements, and maintain the stability of critical branches.	<b>No exceptions noted.</b>
REQ-58	A business continuity and disaster recovery (BC/DR) plan is documented to support continuity and recovery of critical services and business processes after unexpected business interruptions.	Inspected the BC/DR plan to determine that a BC/DR plan was documented to support continuity and recovery of critical services and business processes after unexpected business interruptions.	<b>No exceptions noted.</b>

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-59	The BC/DR plan is tested annually to assess the effectiveness of management's readiness to respond to unexpected business interruptions.	Inspected the BC/DR plan test results to determine that the BC/DR plan was tested annually to assess the effectiveness of management's readiness to respond to unexpected business interruptions.	<b>No exceptions noted.</b>
REQ-60	A Data Backup and Recovery Policy is documented and includes guidance for the Company's data backup and recovery strategy.	Inspected the Data Backup and Recovery Policy to determine that a Data Backup and Recovery Policy was documented and included guidance for the Company's data backup and recovery strategy.	<b>No exceptions noted.</b>
REQ-61	Data backup restoration tests are performed annually to verify data recoverability.	Inspected the data backup restoration test results to determine that data backup restoration tests were performed annually to verify data recoverability.	<b>No exceptions noted.</b>
REQ-62	Daily incremental backups are configured for data stores housing customer data.	Inspected the backup configurations to determine that daily incremental backups were configured for data stores housing customer data.	<b>No exceptions noted.</b>
REQ-63	Data stores are replicated across multiple availability zones to permit the resumption of critical operations in the event of loss of a critical facility.	Inspected the replication configurations to determine that data stores were replicated across multiple availability zones to permit the resumption of critical operations in the event of the loss of a critical facility.	<b>No exceptions noted.</b>
REQ-64	System capacity is evaluated continuously to help ensure that processing capacity can meet demand.	Inspected the system capacity monitoring tool dashboard, configurations and metrics to determine that system capacity was evaluated continuously to help ensure that processing capacity could meet demand.	<b>No exceptions noted.</b>
REQ-65	A Data Classification Policy is documented and includes guidance for the classification and security of confidential data.	Inspected the Data Classification Policy to determine that a Data Classification Policy was documented and included guidance for the classification and security of confidential data.	<b>No exceptions noted.</b>

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-66	Customer data is prohibited by policy from being used or stored in non-production systems or environments.	Inspected the Information Security Policy to determine that customer data was prohibited by policy from being used or stored in non-production systems or environments.	<b>No exceptions noted.</b>
REQ-67	Customer data is purged from the application environment upon customer request.	Inquired of management and inspected the data deletion repository to determine that the circumstances that warrant the operation of the control did not occur during the period.	<b>Not tested. No customer data deletion requests were received during the period. As a result, no operating effectiveness testing could be performed to determine whether customer data was purged from the application environment upon customer request.</b>

## Section 5: Other Information Provided by Patchworks That Is Not Covered by the Service Auditor’s Report

The information included in this section is presented by Patchworks' management to provide additional information and is not a part of Patchworks' description of its Patchworks Platform made available to user entities throughout the period February 1, 2025 to July 31, 2025. Information included in Patchworks' management response to testing exceptions has not been subjected to the procedures applied in the examination and, accordingly, we express no opinion on it.

Management’s Response to Testing Exceptions			
Control No.	Applicable Control Activities	Results of Tests	Management’s Response
REQ-13	Employees and contractors complete security awareness training annually.	Exceptions noted. For 1 of 8 sampled employees and contractors, an annual security awareness training was not completed.	<p>Management acknowledges that the required annual security awareness training was not completed by one sampled personnel, resulting in a deviation from the Company’s security training policy. Upon identification of the exception, management ensured that the affected individual completed the training.</p> <p>While the training was not completed within the designated timeframe, management reinforces security best practices throughout the year via ongoing communications, policy updates, and ad hoc training sessions to promote a strong security culture and maintain user awareness.</p> <p>To help prevent recurrence, management has implemented automated reminders, clarified ownership for tracking training completion, and updated internal procedures to enforce timely completion and documentation of annual training. Management believes these enhancements will strengthen compliance, reduce training gaps, and further integrate security awareness into the Company’s personnel lifecycle.</p>

<b>Management's Response to Testing Exceptions</b>			
<b>Control No.</b>	<b>Applicable Control Activities</b>	<b>Results of Tests</b>	<b>Management's Response</b>
REQ-14	Managers complete performance appraisals for direct reports annually.	Exceptions noted. For 1 of 8 sampled employees and contractors, an annual performance appraisal was not completed.	<p>Management acknowledges that annual performance appraisals were not completed for one sampled direct report during the audit period, resulting in a deviation from the Company's established performance management procedures.</p> <p>Although formal evaluations were not completed in this instance, performance expectations were communicated through regular supervisory oversight, informal feedback, and day-to-day engagement. No issues related to accountability or job performance were identified as a result of the missed appraisals.</p> <p>To remediate this exception and reduce the risk of recurrence, management has implemented a centralized tracking process to monitor the timely completion of performance evaluations. Managers have been reminded of their responsibilities, and evaluations for the affected individuals have since been completed. Going forward, periodic oversight will be conducted to ensure continued compliance with performance management policies. Management believes these actions will strengthen consistency and accountability across the organization.</p>

<b>Management's Response to Testing Exceptions</b>			
<b>Control No.</b>	<b>Applicable Control Activities</b>	<b>Results of Tests</b>	<b>Management's Response</b>
REQ-55	Changes to software and infrastructure components are authorized, documented, tested, reviewed, and approved prior to being implemented in the production environment.	Exceptions noted. For 2 of 20 sampled changes, evidence was not maintained to demonstrate that the changes were approved prior to being implemented in the production environment.	<p>Management acknowledges that evidence was not retained to demonstrate that all sampled changes were approved prior to deployment to the production environment. Although the required steps may have been performed in practice, the absence of supporting documentation limited the ability to validate adherence to the Company's change management procedures. Upon identification of the exception, management conducted a retrospective review of the affected changes and determined that each change was appropriate, operated as intended, and did not result in any production issues or service disruption.</p> <p>To prevent recurrence, management has updated its change management procedures to emphasize the requirement for retaining approval and testing artifacts as part of the change record. Additional training has been provided to the relevant stakeholders, and system-based enforcement has been implemented to require documented evidence before a change can be finalized. These improvements are expected to enhance compliance and traceability across the change management lifecycle.</p>