

## System and Organization Controls (SOC) 2 Type 1 Report for



As of October 31, 2024

Report on Patchworks Media Ltd's description of its Patchworks Platform and on the suitability of the design of its controls relevant to Security, Availability and Confidentiality as of October 31, 2024.

## Table of Contents

- **Section I: Independent Service Auditor's Report Provided by Laika Compliance LLC**
- **Section II: Assertion of Patchworks Media Ltd's Management**
- **Section III: Patchworks' Description of its Patchworks Platform as of October 31, 2024**
- **Section IV: Trust Services Criteria and Related Controls Relevant to the Security, Availability and Confidentiality Categories**

## Section I: Independent Service Auditor's Report Provided by Laika

### Compliance LLC

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 as of October 31, 2024" (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 of controls stated in the description as of October 31, 2024, 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 data center colocation 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.

#### 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's Management" (assertion) about the description and the suitability of design 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 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 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.

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

- 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.
- 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.
- 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 users may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design 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.

### **Other Matter**

We did not perform any procedures regarding the operating effectiveness of controls stated in the description and, accordingly, do not express an opinion thereon.

### **Opinion**

In our opinion, in all material respects—

1. The description presents the Patchworks Platform that was designed and implemented as of October 31, 2024, in accordance with the description criteria.
2. The controls stated in the description were suitably designed as of October 31, 2024, 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 as of that date and if the subservice organization and user entities applied the complementary controls assumed in the design of Patchworks's controls as of that date.

### **Restricted Use**

This report is intended solely for the information and use of Patchworks; user entities of the Patchworks Platform as of October 31, 2024, 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

November 5, 2024

## Section II: Assertion of Patchworks Media Ltd's Management

We have prepared the accompanying description of the Patchworks Platform "Patchworks' Description of its Patchworks Platform as of October 31, 2024" (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 the Patchworks Platform, 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 data center colocation 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—

1. The description presents the Patchworks Platform that was designed and implemented as of October 31, 2024, in accordance with the description criteria.
2. The controls stated in the description were suitably designed as of October 31, 2024, 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 as of that date, and if the subservice organization and user entities applied the complementary controls assumed in the design of Patchworks' controls as of that date.

Patchworks Media Ltd

## Section III: Patchworks' Description of its Patchworks Platform as of October 31, 2024

### 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 Data Processing Agreement (DPA), Terms of Service and Service Level Objectives include the communication of the Company's commitments to its customers. Changes to any commitments are communicated to 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
<b>Security</b>	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.	<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 Container Registry (ECR)	Container Registry	AWS
Amazon Elastic Kubernetes Service (EKS)	Container Orchestration	AWS
Amazon GuardDuty	Threat Detection	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 CloudWatch	Infrastructure Monitoring
Amazon Inspector	Vulnerability Scanning
AWS Identity Access Management (IAM)	Identity and Access Management
Cloudflare	Domain Name Service
GitHub	Code Repository

Software	
Production Application	Business Function
Google Workspace	Single Sign-On (SSO) and Authentication
Grafana	Infrastructure Monitoring
Jira	Ticketing System
LastPass	Password Management
NordLayer	Virtual Private Network
Slack	Alert Communication
Terraform	Configuration Management

**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 customer relationships.
Engineering	Responsible for the development, testing, deployment, and maintenance of new code.
Executive Management	Responsible for overseeing company-wide activities, establishing and accomplishing goals, and managing objectives.
Marketing	Responsible for marketing, brand awareness, and lead generation.
People	Responsible for onboarding new personnel, defining the roles and positions of new hires, performing background checks, and facilitating the employee termination process.

People	
Group/Role Name	Function
Product	Responsible for gathering requirements for product features and enhancements.
Sales	Responsible for sales and marketing.

**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.
Data Classification and Handling	How the Company classifies data included in the service and the procedures for handling the data.

Procedure	Description
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 or 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 as of October 31, 2024.

**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. The Code of Conduct describes employee responsibilities and expected behavior regarding data and information system usage. Employees 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 has documented oversight 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, background 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 processing, 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. Internal network vulnerability scans are performed continuously 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.

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 formally 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 employees upon hire. In the event of a significant change to the Information Security Policy, a communication is sent to all new and existing employees 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

Access management processes exist so that Patchworks employee user accounts are added, modified, or disabled in a timely manner and are reviewed on a semi-annual basis. In addition, password configuration settings for user authentication to the Patchworks Platform are managed in compliance with Patchworks' Password Policy which is part of the Information Security Policy.

Users must be approved for logical access by management prior to receiving access to the Patchworks Platform. Management authorization is required before employment is offered and access is provided. Users must also be assigned a unique ID before being allowed access to system components. User IDs are authorized and implemented as part of the new hire on-boarding process. Access rights and privileges are granted to user IDs based on the principle of least privilege and Role-Based Access Control (RBAC) protocols. Access is limited to that which is required for the performance of job duties for individual users, and generic access by Patchworks employees is not allowed.

## SYSTEM OPERATIONS

An Incident Response Policy and Procedures manual has been formally 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 Configuration and Change Management Policy has been formally 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 formally documented and implemented to ensure that all systems and network devices are properly and securely configured. Center for Internet Security (CIS) and National Institute of Technology (NIST) hardening standards, as well as configurations in AWS are used as a basis for Patchworks' system configuration standards.

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

Patchworks uses AWS to host the Patchworks Platform. Patchworks uses multiple availability zones (AZ's) to allow the resumption of service in the case of an AZ outage. The Engineering Team is responsible for performing daily incremental backups of the Patchworks Platform including application data, critical data necessary to resume the in-scope services, customer data and sensitive data. The Engineering Team monitors backups for any errors using logging tools and uses notification tools to alert the team if an error is triggered and action is required to be taken.

## 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 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 data center colocation 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 colocation services for IT infrastructure 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. CSOCs are expected to be in place at AWS related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. AWS physical security controls should mitigate the risk of unauthorized access to the hosting facility. AWS environmental protection controls should mitigate the risk of fires, power loss, climate, and temperature variability.

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)
CC6.4	<ul style="list-style-type: none"> <li>• AWS is responsible for restricting data center access to authorized personnel.</li> <li>• AWS is responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel.</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.</li> </ul>
CC7.2 A1.2	<ul style="list-style-type: none"> <li>• AWS is responsible for the installation of fire suppression and detection and environmental monitoring systems at the data centers.</li> <li>• AWS is responsible for protecting data centers against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS).</li> <li>• AWS is responsible for overseeing the regular maintenance of environmental protections at data centers.</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.

**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 IV: Trust Services Criteria and Related Controls Relevant to the Security, Confidentiality, and Availability

### Categories

This SOC 2 Type 1 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 of controls stated in the description as of October 31, 2024. This section of the report includes 2 tables:

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

Table 2: Description of the Applicable Control Activities

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

CC1.0 - Control Environment		
Criteria	Applicable Control Activities	Criteria Description
CC1.1	LCL-1 LCL-2 LCL-3 LCL-10	The entity demonstrates a commitment to integrity and ethical values.
CC1.2	LCL-4 LCL-5	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
CC1.3	LCL-5 LCL-6 LCL-7 LCL-8	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
CC1.4	LCL-8 LCL-9 LCL-10	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

<b>CC1.0 - Control Environment</b>		
<b>Criteria</b>	<b>Applicable Control Activities</b>	<b>Criteria Description</b>
CC1.5	LCL-1 LCL-8 LCL-10	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

<b>CC2.0 - Information and Communication</b>		
<b>Criteria</b>	<b>Applicable Control Activities</b>	<b>Criteria Description</b>
CC2.1	LCL-5 LCL-18 LCL-22 LCL-46 LCL-47 LCL-48	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.
CC2.2	LCL-7 LCL-8 LCL-9 LCL-12	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
CC2.3	LCL-13 LCL-14 LCL-15	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	LCL-16 LCL-17	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

CC3.0 - Risk Assessment		
Criteria	Applicable Control Activities	Criteria Description
CC3.2	LCL-17 LCL-18 LCL-58	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	LCL-17 LCL-18	The entity considers the potential for fraud in assessing risks to the achievement of objectives.
CC3.4	LCL-17 LCL-18 LCL-19 LCL-20 LCL-21	The entity identifies and assesses changes that could significantly impact the system of internal control.

CC4.0 - Monitoring Activities		
Criteria	Applicable Control Activities	Criteria Description
CC4.1	LCL-5 LCL-18 LCL-20 LCL-21 LCL-22 LCL-46 LCL-47 LCL-55	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	LCL-5 LCL-18 LCL-22 LCL-55	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.

CC5.0 - Control Activities		
Criteria	Applicable Control Activities	Criteria Description
CC5.1	LCL-17 LCL-22	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
CC5.2	LCL-17 LCL-22	The entity also selects and develops general control activities over technology to support the achievement of objectives.
CC5.3	LCL-17 LCL-23 LCL-24 LCL-25 LCL-26 LCL-27 LCL-28 LCL-29 LCL-30 LCL-60 LCL-62	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	LCL-31 LCL-32 LCL-33 LCL-34 LCL-35 LCL-39 LCL-54	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.

CC6.0 - Logical and Physical Access		
Criteria	Applicable Control Activities	Criteria Description
CC6.2	LCL-36 LCL-37 LCL-38	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
CC6.3	LCL-36 LCL-37 LCL-38	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>N/A: The Company's production environment is hosted at third-party data centers, which are carved out for the 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	LCL-30 LCL-39	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	LCL-40 LCL-41 LCL-42 LCL-43 LCL-44	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
CC6.7	LCL-44 LCL-48	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	LCL-43 LCL-48	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	LCL-18 LCL-19 LCL-46 LCL-47	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.
CC7.2	LCL-20 LCL-21 LCL-42 LCL-43 LCL-46 LCL-47 LCL-48 LCL-49	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	LCL-20 LCL-21 LCL-23 LCL-46 LCL-47 LCL-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	LCL-23 LCL-43 LCL-51 LCL-52	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	LCL-23 LCL-51 LCL-52 LCL-58	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	LCL-43 LCL-53 LCL-54	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	LCL-17 LCL-23 LCL-52 LCL-58 LCL-59	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.
CC9.2	LCL-14 LCL-55	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	LCL-49 LCL-56	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	LCL-57 LCL-58 LCL-59 LCL-60	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	LCL-58 LCL-60 LCL-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	LCL-14 LCL-30 LCL-62 LCL-63	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.
C1.2	LCL-64	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.

## Table 2: Description of the Applicable Control Activities

Control activities tested in connection with determining the design of controls relative to the applicable Trust Services Criteria are described below.

Control #	Applicable Control Activities
LCL-1	Upon hire, employees acknowledge that they have read and agree to a code of conduct that describes their responsibilities and expected behavior regarding data and information system usage.
LCL-2	Employees sign a confidentiality agreement upon hire. This agreement prohibits any disclosure of information and other data to which the employee has been granted access.
LCL-3	New personnel offered employment are subject to background checks prior to their start date.
LCL-4	The Risk Committee has documented oversight responsibilities relative to internal control. The Risk Committee includes members that are independent of the internal control function.
LCL-5	The Risk Committee meets quarterly and maintains formal meeting minutes.
LCL-6	An organization chart is documented and defines the organizational structure and reporting lines.
LCL-7	Management has established defined roles and responsibilities to oversee the implementation of the security and control environment.
LCL-8	Job descriptions are documented for employees supporting the service and include authorities and responsibilities in support of the system.
LCL-9	Employees complete security awareness training upon hire and annually thereafter.
LCL-10	Managers complete performance appraisals for direct reports annually.
LCL-12	System changes are communicated to authorized internal users.
LCL-13	The Data Processing Agreement (DPA), Terms of Service and Service Level Objectives include the communication of the Company's commitments to its customers.
LCL-14	Formal information sharing agreements are in place with critical vendors. These agreements include confidentiality commitments applicable to that entity.
LCL-15	Technical support resources related to system operations are provided on the Company's website.
LCL-16	The Company specifies its objectives in its annual risk assessment to enable the identification and assessment of risk related to the objectives.
LCL-17	A documented risk assessment policy is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.
LCL-18	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.
LCL-19	A configuration management tool is in place to ensure that system configurations are deployed consistently throughout the environment.
LCL-20	Penetration testing is performed annually to identify vulnerabilities that could be exploited to gain access to the production environment.
LCL-21	A remediation plan is developed and changes are implemented to remediate, at a minimum, all critical and high vulnerabilities identified during the annual penetration test.
LCL-22	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.
LCL-23	An incident response policy is documented and provides guidance for detecting, responding to, and recovering from security events and incidents. The policy is made available to users.

Control #	Applicable Control Activities
LCL-24	Formal procedures are documented that outline the process the Company's staff follows to perform the following access control functions: <ul style="list-style-type: none"> <li>- Adding new users</li> <li>- Modifying an existing user's access</li> <li>- Removing an existing user's access</li> <li>- Restricting access based on separation of duties and least privilege</li> </ul>
LCL-25	An information security policy is documented and defines the information security rules and requirements for the service environment. The policy is reviewed annually.
LCL-26	Formal procedures are documented that outline requirements for vulnerability management and system monitoring. The procedures are reviewed annually.
LCL-27	A vendor management program is in place. Components of this program include: <ul style="list-style-type: none"> <li>- Maintaining a list of critical third-party vendors</li> <li>- Requirements for third-party vendors to maintain their own security practices and procedures</li> <li>- Annually reviewing critical third-party attestation reports or performing a vendor risk assessment</li> </ul>
LCL-28	A formal change management methodology is in place that governs documentation, testing, review, and approval of changes to information systems.
LCL-29	Hardening standards are documented and reviewed annually.
LCL-30	Formal data retention and disposal procedures are in place to guide the secure retention and disposal of customer data.
LCL-31	Authentication to the following in-scope production system components requires a username and password combination: <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>- Firewalls</li> <li>- Encryption keys</li> <li>- Code Repository</li> </ul>
LCL-32	Privileged access to the following in-scope production 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>- Firewalls</li> <li>- Encryption Keys</li> <li>- Code Repository</li> </ul>
LCL-33	Passwords for in-scope production system components are configured according to the password policy.
LCL-34	The network is segmented to prevent unauthorized access to customer data.

Control #	Applicable Control Activities
LCL-35	Encryption is enabled for data stores housing sensitive customer data.
LCL-36	User access to in-scope system components is based on job role and function and requires a documented access request and manager approval prior to access being provisioned.
LCL-37	Access to system components is revoked within 24 hours of termination as part of the termination process.
LCL-38	Semi-annual access reviews are conducted by management for the in-scope system components to help ensure that access is restricted appropriately. The review is documented, and access is modified or removed where applicable.
LCL-39	An inventory of production system assets is maintained by management.
LCL-40	Remote access to production infrastructure and cloud consoles is restricted to authorized users with valid multi-factor authentication (MFA) tokens.
LCL-41	AWS security groups are used and configured to prevent unauthorized access to the production environment.
LCL-42	An intrusion detection system (IDS) is used to provide continuous monitoring of the Company's network and early detection of potential security breaches.
LCL-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.
LCL-44	Secure data transmission protocols are used to encrypt customer data when transmitted over public networks.
LCL-46	Internal network vulnerability scans are performed continuously to identify, quantify, and prioritize vulnerabilities.
LCL-47	Changes are implemented to remediate, at a minimum, all critical and high vulnerabilities identified during continuous internal network vulnerability scans.
LCL-48	A log management tool is utilized to monitor and identify events that may have a potential impact on the Company's ability to achieve its security objectives. Alerts are configured to notify IT personnel upon identification of such security events to allow for further triage where necessary.
LCL-49	An infrastructure monitoring tool is utilized to monitor infrastructure availability and performance and generates alerts when specific, predefined thresholds are met.
LCL-51	All incidents related to security are logged, tracked, evaluated and communicated to affected parties by management until the Company has recovered from the incidents.
LCL-52	The incident response plan is tested annually to assess the effectiveness of the incident response program.
LCL-53	Changes to software and infrastructure components of the service are authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.
LCL-54	Access to migrate changes to production is restricted to authorized personnel.
LCL-55	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.
LCL-56	System capacity is evaluated continuously to help ensure that processing capacity can meet demand.
LCL-57	Daily incremental backups are configured for data stores housing customer data.
LCL-58	A documented business continuity/disaster recovery (BC/DR) plan is in place and tested annually.
LCL-59	Data stores are replicated across multiple availability zones to permit the resumption of critical operations in the event of loss of a critical facility.
LCL-60	Procedures are documented that outline the Company's data backup and recovery strategy.
LCL-61	Data backup restoration tests are performed annually to verify data recoverability.
LCL-62	A data classification policy is in place to help ensure that confidential data is properly secured and restricted to authorized personnel.
LCL-63	Customer data is prohibited by policy from being used or stored in non-production systems or environments.

Control #	Applicable Control Activities
LCL-64	Customer data is purged from the application environment upon request when customers leave the service.