# All Day TA

# SOC 2 TYPE 2 REPORT

## FOR THE PERIOD FEBRUARY 15, 2025 to AUGUST 15, 2025

A TYPE 2 INDEPENDENT SERVICE AUDITOR'S REPORT ON
CONTROLS RELEVANT TO
SECURITY, CONFIDENTIALITY, AND AVAILABILITY

---

**AUDIT AND ATTESTATION BY**

AT&F International, Inc.
*your global partner to thrive your business*

**AICPA NOTICE:**

You may use the SOC for Service Organizations - Service Organizations Logo only for a period of twelve (12) months following the date of the SOC report issued by a licensed CPA. If after twelve months a new report is not issued, you must immediately cease use of the SOC for Service Organizations - Logo.

# TABLE OF CONTENTS

# SECTION 1

MANAGEMENT'S ASSERTION

# Management Assertion

We have prepared the accompanying description of All Day TA ("All Day TA" or the company) system throughout the period February 15, 2025 to August 15, 2025, based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report. The description is intended to provide report users with information about All Day TA system that may be useful when assessing the risks arising from interactions with All Day TA system, particularly information about system controls that All Day TA 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, Confidentiality, and Availability set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.*

All Day TA uses AWS as a subservice organization for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at All Day TA, to achieve All Day TA's service commitments and system requirements based on the applicable trust services criteria. The description presents All Day TA controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of All Day TA 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 All Day TA, to achieve All Day TA service commitments and system requirements based on the applicable trust services criteria. The description presents All Day TA controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of All Day TA controls.

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

a) The description presents All Day TA systems that were designed and implemented throughout the period February 15, 2025 to August 15, 2025, in accordance with the description criteria.

b) The controls stated in the description were suitably designed throughout the period February 15, 2025 to August 15, 2025, to provide reasonable assurance that All Day TA's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period, and if the subservice organization and user entities applied the complementary controls assumed in the design of All Day TA's controls during that period.

c) The controls stated in the description operated effectively throughout the period February 15, 2025 to August 15, 2025, to provide reasonable assurance that All Day TA's service commitments and system requirements were achieved based on the applicable trust services criteria, if the complementary subservice organization and complementary user entity controls assumed in the design of All Day TA's controls operated effectively throughout the period.

Chelsea Kerr
Director
All Day TA

# SECTION 2

## INDEPENDENT SERVICE AUDITOR'S REPORT

# Independent Service Auditor's Report

To: All Day TA

## Scope

We have examined All Day TA ("All Day TA") accompanying description of its various systems found in Section 3, titled All Day TA System Description throughout the period February 15, 2025 to August 15, 2025, based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report, and the suitability of the design and operating effectiveness of controls stated in the description throughout the period February 15, 2025 to August 15, 2025, to provide reasonable assurance that All Day TA service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Confidentiality, and Availability set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.*

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

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

## Service Organization's Responsibilities

All Day TA 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 All Day TA service commitments and system requirements were achieved. In Section 1, All Day TA has provided the accompanying assertion titled "Management's Assertion of All Day TA" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. All Day TA 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 the 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 AICPA. 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.

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

1. Obtaining an understanding of the system and the service organization's service commitments and system requirements.
2. 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.
3. Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
4. Performing procedures to obtain evidence about whether controls stated in the description were suitably designed and implemented to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
5. 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.
6. Evaluating the overall presentation of the description.

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

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

## Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report 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. 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 Test of Controls

The specific controls tested and the nature, timing, and results of those tests are presented in the section of our report titled "Testing Matrices."

## Opinion

In our opinion, in all material respects:

a) The description presents the All Day TA system that was designed and implemented throughout the period February 15, 2025 to August 15, 2025, in accordance with the description criteria.

b) The controls stated in the description were suitably designed throughout the period February 15, 2025 to August 15, 2025, to provide reasonable assurance that All Day TA's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period and if the subservice organization and user entities applied the complementary controls assumed in the design of All Day TA's controls throughout the period.

c) The controls stated in the description operated effectively throughout the period February 15, 2025 to August 15, 2025, to provide reasonable assurance that All Day TA's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of All Day TA's controls operated effectively throughout the period.

## Restricted Use

This report is intended solely for the information and use of All Day TA, user entities of All Day TA system during some or all of the period February 15, 2025 to August 15, 2025, business partners of All Day TA subject to risks arising from interactions with the system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

1. The nature of the service provided by the service organization.
2. How the service organization's system interacts with user entities, business partners, and other parties.
3. Internal control and its limitations.
4. Complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
5. User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
6. The applicable trust services criteria.
7. 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.

AT & F International

Digitally signed by AT and F International, Inc
Date: 2025.09.30 01:11:10 +05'30'

AT and F International, Inc.,
Wilmington, Delaware
Firm License No.: CF-0010900

# SECTION 3

SYSTEM DESCRIPTION

# DC 1: Company Background

# Overview of Operations

**Description of Services Provided**

All Day TA is an AI EdTech company focused on higher education that enables professors to build customized AI teaching assistants for their courses. Available 24/7, it provides students with instant, accurate answers to any course-related question.

**Mission & Vision**

All Day TA seeks to revolutionize education by providing students with the experience of having a personal tutor using AI. Starting with our AI Assistant, we will provide students with a 24/7 study companion, we will build upon that experience to deliver personalized questions and exercises to help students improve their understanding at their own pace and focusing on areas where understanding is weaker.

# DC 2: Principal service commitments and system requirements

All Day TA designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that All Day TA makes to user entities, the laws and regulations that govern its services, and the financial, operational, and compliance requirements that All Day TA has established. The system services are subject to the security, confidentiality, and availability commitments established internally for its services.

Commitments to user entities are documented and communicated in service-level agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online.

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

- The fundamental design of All Day TA's software application addresses security concerns such that system users can access the information based on their role in the system and are restricted from accessing information not needed for their role.
- All Day TA implements various procedures and processes to control access to the production environment and the supporting infrastructure.
- Monitoring of key infrastructure components is in place to collect and generate alerts based on utilization metrics.
- Operational procedures for managing security incidents and breaches, including notification procedures.

Confidentiality commitments include, but are not limited to, the following:

- The use of encryption technologies to protect system data both at rest and in transit.
- Confidentiality and non-disclosure agreements with employees, contractors, and third parties; and,
- Confidential information must be used only for the purposes explicitly stated in agreements between All Day TA and user entities.

Availability commitments include, but are not limited to, the following:

- System performance and availability monitoring mechanisms to help ensure the consistent delivery of the system and its components.
- Responding to customer requests in a timely manner.
- Business continuity and disaster recovery plans and,
- Operational procedures supporting the achievement of availability commitments to user entities.

Such requirements are communicated in All Day TA's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures are documented on how to carry out specific manual and automated processes required in the operation and development of the system.

# DC 3: Components of the System used to provide services

The purpose of the system description is to delineate the boundaries of the system, which includes the services and commitments outlined above and the five components described below:

## 3.1 Infrastructure

The All Day TA is hosted in Amazon Web Services in their US East 1 - N. Virginia region. All Day TA's software application uses a virtual and secure network environment on top of AWS infrastructure to ensure that the software application is always protected. This is achieved by hosting the application inside a virtual private cloud (VPC) and accompanying firewalls on the infrastructure provider.

All Day TA software application ensures there are only specific authorized points of entry, and filters traffic to the private networks that support the application.

When a customer's client device connects to the application over the internet, their data is encrypted and secured over HTTPS. It then passes through an AWS Internet Gateway, over to a virtual private cloud that:

- Houses the entire application runtime
- Protects the application runtime from any external networks

The internal networks of AWS are protected by deny-by-default security groups and firewalls to ensure that only deliberately allowed traffic can pass through.

Further, all VPC network flow logs, DNS logs, and other AWS console events are continuously monitored by AWS Guard duty to spot malicious activity and unauthorized behavior. Specifically, AWS Guard duty uses machine learning, anomaly detection, and integrated threat intelligence to identify potential threats

## 3.2 Software

All Day TA is responsible for managing the development and operation of the All Day TA including infrastructure components such as servers, databases, and storage systems. The in-scope All Day TA infrastructure and software components are shown in the table below:

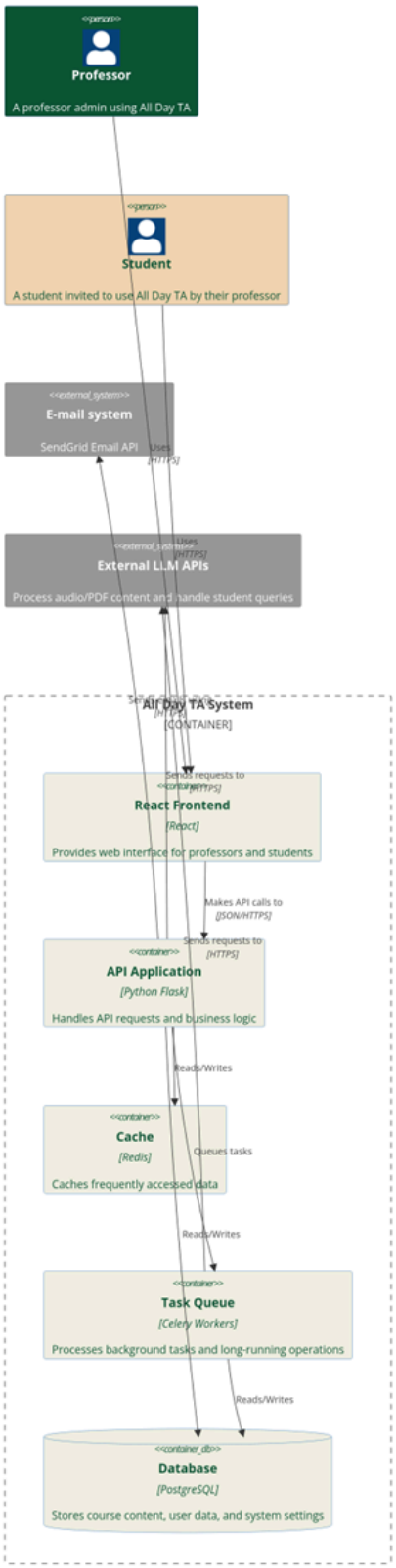
| Primary Infrastructure and Software | | |
|---|---|---|
| **System / Application** | **Business Function / Description** | **Physical Location** |
| React Frontend | Provides web interface for professors and students | Amazon Web Services in their US East 1 - N. Virginia region |
| API Application | Handles API requests and business logic | Amazon Web Services in their US East 1 - N. Virginia region |
| Cache | Caches frequently accessed data | Amazon Web Services in their US East 1 - N. Virginia region |
| Task Queue | Processes background tasks and long-running operations | Amazon Web Services in their US East 1 - N. Virginia region |

| | | |
|---|---|---|
| Database | Stores course content, user data, and system settings | Amazon Web Services in their US East 1 - N. Virginia region |

| Supporting Tools | |
|---|---|
| **System / Application** | **Business Function / Description** |
| E-mail system | SendGrid Email API |
| External LLM APIs | Process audio/PDF content and handle student queries |

**Network Architecture Diagram -**

Container diagram for All Day TA



## 3.3 People

All Day TA's staff have been organized into various functions like Sales, Support, Engineering, Product Management etc. The personnel have also been assigned the following key roles:

**Senior Management:** Senior management carries the ultimate responsibility for achieving the mission and objectives of the organization. They ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the organization's mission. They also assess and incorporate results of the risk assessment activity into the decision-making process. The senior management understands that their support and involvement is required in order to run an effective risk management program that assesses and mitigates IT-related mission risks.

**Information Security Officer:** The Senior Management assigns the role of Information Security Officer to one of its staff members who is responsible for the performance of the information security program of the organization. Decisions made in these areas are based on an effective risk management program. The Information Security Officer is responsible for identifying risks, threats, vulnerabilities, and adding controls to mitigate this risk. Additionally, they also summarize remaining residual risks and report the same to Senior Management in a timely manner.

**Compliance Program Manager**: The company assigns the role of Compliance Program Manager to a staff member who would be responsible for the smooth functioning of the Information Security Program. The Compliance Program Manager takes care of effective and timely completion of tasks required for the functioning of all information security controls, across all functions/departments of the organization.

**System Users:** The organization's staff members are the users of the IT systems. The organization understands that use of the IT systems and data according to an organization's policies, guidelines, and rules of behavior is critical to mitigating risk and protecting the organization's IT resources. To minimize risk to the IT systems, staff members that access IT resources are provided with annual security awareness training.

## 3.4 Data

Data, as defined by All Day TA, constitutes the following:

- Error logs
- System files
- Input reports
- Output reports
- Electronic interface files
- Transaction data

Output reports are available upon request and include data and files systematically generated from the system. The availability of these reports is limited by job function. Reports delivered externally are only sent using a secure method—encrypted email, secure FTP, or secure websites to customer users.

All data that is managed, processed and stored as a part of the All Day TA software application is classified as per the Data Classification Policy which establishes a framework for categorizing data based on its sensitivity, value and criticality to achieving the objectives of the organization.

All customer data is categorized as confidential. Further, all customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer contracts. All data is to be assigned one of the following sensitivity levels:

Customer data is retained per agreements with customers and disposed of upon request by customers. A confirmation is sent back to the customer to notify them that the disposal is complete.

## Procedures and Policies

Formal policies and procedures have been established to support the All Day TA software application. These policies cover:

- Code Of Conduct Policy
- Acceptable Use Policy
- Access Control Policy
- Asset Management Policy
- Backup And Restoration Policy
- Password Policy
- Data Classification Policy
- Incident Management Policy
- Information Security Policy
- Software Development Policy
- Data Retention And Deletion Policy
- Physical Security Policy
- Third-Party Risk Management Policy
- Responsible Disclosure Policy

- Data Protection Policy
- Key Management And Cryptography Policy
- Risk Assessment Policy
- Vulnerability Management Policy
- Business Continuity And Disaster Recovery Policy

All policies are made available to all staff members to provide direction regarding the staff members' responsibilities related to the functioning of internal control. All staff members are expected to adhere to the policies and procedures that define how services should be delivered. Specifically, staff members are required to acknowledge their understanding of these policies upon hiring (and annually thereafter).

All Day TA also provides information to clients and staff members on how to report failures, incidents, concerns, or complaints related to the services or systems provided by the All Day TA software application, in the event there are problems, and takes actions within an appropriate timeframe as and when issues are raised.

## DC 4: Disclosures about identified security incidents

No significant incidents have occurred to the services provided to user entities in the last 12 months preceding the end of the review date.

## DC 5: Relevant aspects of the Control Environment, Risk Assessment Process, Information and Communication, and Monitoring

The applicable trust services criteria were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. Although the applicable trust services criteria and related controls are included in Section IV, they are an integral part of All Day TA's description of the system. This section provides information about the five interrelated components of internal control at All Day TA, including:

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring controls

### *Control Environment*

## Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of All Day TA's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of All Day TA's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct.

All Day TA and its management team has established the following controls to incorporate ethical values throughout the organization:

- A formally documented "Code of Conduct Policy" communicates the organization's values and behavioral standards to staff members
- Staff members are required to acknowledge (upon hiring and annually thereafter) comprehensive policies and procedures covering the areas of Information Security, Change Management, Incident Management and Access Control. Staff Members also acknowledge that they understand their responsibility for adhering to the policies and procedures.
- All new employees go through background checks as a part of the hiring process, with the exception of co-op interns who provide proof of citizenship and enrolment.

## Commitment to Competence

All Day TA's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. The following controls have been established in order to incorporate the commitment to competence throughout the organization:

- Management outlines the roles and responsibilities of technical staff to ensure that they are clear about their responsibilities in the organization. These roles and responsibilities are reviewed annually by the senior management.
- Annual Security Awareness Training is provided to all staff which focuses on maintaining the security of the proprietary and customer-servicing systems and related data.
- Employees receive periodic reviews by their supervisors inclusive of discussing any deficiencies noted in the execution of their job responsibilities.
- Employees are evaluated for competence in performing their job responsibilities at the time of hiring.

**Senior Management Oversight**

All Day TA's control awareness is significantly influenced by its senior management. Attributes that define "tone at the top" include senior management's experience of its members, their involvement and scrutiny of operational activities, and their interaction with independent assessments of the company's operations and information security posture.

## Management Philosophy and Operating Style

All Day TA's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to monitoring business risks, and management's attitudes toward personnel and the processing of information. All Day TA's control environment reflects the philosophy of management. All Day TA's information security function, composed of senior management and the Information Security Officer, meets frequently and includes at least an annual meeting to review policies and procedures and set the information security program roadmap. The security function, under the direction of senior management, oversees the security activities and communication of its policies and procedures.

Specific control activities All Day TA has implemented in this area are described below:

- Senior management meetings are held to discuss major initiatives and issues that affect the business as a whole.
- Senior management reviews the functioning of internal controls, vendor risk assessment, risk assessment, and high severity security incidents annually.
- Senior management meets frequently and includes at least an annual meeting to review policies and procedures and set the information security program roadmap.

## Organizational Structure and Assignment of Authority and Responsibility

All Day TA's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

The management is committed to maintaining and improving its framework for how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. This also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties.

In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable. Organizational charts are in place to communicate key areas of authority and responsibility. These charts are accessible to all employees of the company and updated as required.

### Human Resources

All Day TA's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by the management's ability to hire and retain top quality personnel who ensure the service organization operates at maximum efficiency.

Specific control activities that the service organization has implemented in this area are described below:

- Background checks are performed on new hires, who are evaluated for competence in performing their job responsibilities at the time of hiring.
- Job positions are supported by job descriptions.
- New employees are required to acknowledge company policy and confidentiality related agreements upon hire and annually thereafter.
- Upon hire and annually thereafter, all employees must complete training courses covering basic information security practices.
- Performance evaluations for each employee are performed on an annual basis.
- If an employee violates the Code of Conduct in the employee handbook or the company's
- Policies, or otherwise acts in a manner deemed contrary to the mission and objectives of the company, the employee is subject to sanctions up to and including termination of employment.

## *Risk Assessment*

All Day TA regularly reviews the risks that may threaten the achievement of its service commitments and system requirements related to the 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).

All Day TA's risk assessment process identifies significant risks inherent in products and services as they oversee their areas of responsibility. All Day TA identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process identifies risks to the services provided by the All Day TA software application, and management has implemented various measures designed to manage these risks.

All Day TA believes that effective risk management is based on the following principles:

- Senior management's commitment to the security of All Day TA software application
- The involvement, cooperation, and insight of all All Day TA staff

- Initiating risk assessments with discovery and identification of risks
- Thorough analysis of identified risks
- Commitment to the strategy and treatment of identified risks
- Communicating all identified risks to the senior management
- Encouraging all All Day TA staff to report risks and threat vectors

## Scope

The risk assessment and management program applies to all systems and data that are a part of the All Day TA software application. The All Day TA risk assessment exercise evaluates infrastructure such as computer infrastructure, containing networks, instances, databases, systems, storage, and services. The risk assessments also include an analysis of business/IT practices, procedures, and physical spaces as needed.

Risk assessments may be high level or detailed to a specific organizational or technical change as the stakeholders and technologists see fit.

Overall, the execution, development, and implementation of risk assessment and remediation programs is the joint responsibility of All Day TA's Information Security Officer and the department or individuals responsible for the area being assessed. All All Day TA staff are expected to cooperate fully with any risk assessment being conducted on systems and procedures for which they are responsible. Staff are further expected to work with the risk assessment project lead in the development of a remediation plan per risk assessment performed.

## Vendor Risk Assessment

All Day TA uses a number of vendors to meet its business objectives. All Day TA understands that risks exist when engaging with vendors and as a result, continuously assesses those risks that could potentially affect the Company's ability to meet its business objectives.

All Day TA employs several activities to effectively manage their vendors. Firstly, the Information Security Officer performs an annual exercise of thoroughly examining the nature and extent of risks involved with each vendor relationship. For critical vendors, All Day TA assesses vendor compliance commitments through the review of available information security assessment reports and determines whether compliance levels adequately support All Day TA's commitments to its customers. If a critical vendor is unable to provide a third-party security report or assessment, All Day TA management meets with such vendors periodically to assess their performance, security concerns, and their services. Any vendor risks identified are recorded in the risk assessment matrix, which is reviewed annually by the Senior Management of the company.

## Integration with Risk Assessment

As part of the design and operation of the system, All Day TA identifies the specific risks that service commitments may not be met, and designs controls necessary to address those risks. All Day TA's management performs an annual Risk Assessment Exercise to identify and evaluate internal and external risks to the Company, as well as their potential impacts, likelihood, severity and mitigating action.

## *Control Activities*

All Day TA's control activities are defined through its established policies and procedures which address individual risks associated with the achievement of the company's objectives. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions.

Policies serve as the basis for procedures. Control activities are deployed through policies that establish what is expected and procedures that put policies into action.

**Logical Access Control**

The All Day TA software application uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. User access, which is role-based, is controlled in the software application and authenticates to the database.

All Day TA has identified certain systems that are critical to meet its service commitments. All access to critical systems is under the principle of least required privilege (wherein a staff member is granted the minimum necessary access to perform their function) and controlled by the role of the staff member as well as a role based access matrix prior to being issued system credentials and granted the ability to access the system. When a person is relieved of duties from the company, access to critical systems are revoked within three business days.

Administrator access to the production console is restricted to authorized system and security administrators. Powerful service/system accounts and keys are either restricted from direct user authentication or authorized to unique users through a password vault or equivalent security solution. Production infrastructure root level account usage is logged with alerting configured.

The Information Security Officer is responsible for performing quarterly reviews of everyone who has access to the system and assesses the appropriateness of the access and permission levels and make modifications based on the principle of least-privilege, whenever necessary.

Staff members must use complex passwords, wherever possible, for all of their accounts that have access to All Day TA customer data. Staff are encouraged to use passwords which have at least 12 characters, randomly generated, alphanumeric and special-character based. Password configuration settings are documented and systematically enforced based on the password complexity requirements configured on each critical system. Access to cloud services or remote access systems requires multi-factor authentication (MFA).

Additionally, company owned endpoints are configured to auto-screen-lock after 15 minutes of inactivity.

#### Physical Access and Environmental Controls

The in-scope system and supporting infrastructure is hosted by AWS. As such, AWS is responsible for the physical security controls of the in-scope system. All Day TA reviews the SOC 2 report provided by AWS on an annual basis, to ensure their controls are in accordance with standards expected by the customers of the All Day TA software application.

#### Incident Management

All Day TA has an incident management framework that includes defined processes, roles, communications, responsibilities, and procedures for detection, escalation, and response to incidents internally and to customers. Customers are directed to contact All Day TA via the support email address provided during onboarding to report failures, incidents, concerns, or other complaints in the event there were problems.

Incident response procedures and centralized tracking tools consist of different channels for reporting production system incidents and weaknesses. Production infrastructure is configured to generate audit events for actions of interest related to operations and security. Security alerts are tracked, reviewed, and analyzed for anomalous or suspicious activity.

Where required, security incidents are escalated to privacy, legal, customer, or senior management team(s) and assigned a severity rating. Operational events are automatically resolved by the self-healing system.

- **Low severity incidents** are those that do not require immediate remediation. These typically include a partial service of All Day TA being unavailable (for which workarounds exist). These do not require someone to be paged or woken up beyond normal work hours.

- **Medium severity incidents** are similar to low but could include scenarios like suspicious emails or unusual activity on a staff laptop. Again, these do not require immediate remediation or trigger automatic calls outside work hours. Low and medium severity incidents usually cover the large majority of incidents found.

- **High severity incidents** are problems an active security attack has not yet happened but is likely. This includes situations like backdoors, malware, malicious access of business data (e.g., passwords, payment information, vulnerability data, etc.). In such cases, the information security team must be informed and immediate remediation steps should begin.

- **Critical severity incidents** are those where a security attack was successful and something important was lost (or irreparable damage caused to production services). Again, in such cases, immediate actions need to be taken to limit the damage.

Post-mortem activities are conducted for incidents with critical severity ratings. Results of post-mortems may include updates to the security program or changes to systems required as a result of incidents.

**Network Operations Monitoring**

Web applications are protected by deploying network firewalls and security groups that inspect traffic flowing to the web application for common attacks. The network is segmented based on the label or classification level of the information stored on the servers. This includes filtering between virtual private cloud (VPC) environments to help ensure only authorized systems are able to communicate with other systems necessary to fulfill their specific responsibilities. Operations and security functions use a variety of security utilities to identify and detect possible security threats and incidents. These utilities include, but are not limited to, firewall notifications, intrusion detection system (IDS) or intrusion prevention system (IPS) alerts, vulnerability assessment reports, and operating system event logs.

Incidents and alerts from the security utilities are reviewed by All Day TA management. Security events requiring further investigation are tracked using internal ticketing systems and monitored until resolved.

All Day TA only uses network ports, protocols, and services listening on a system with validated business need to run on each system. Default-deny rules drop traffic except those services and ports that are explicitly allowed.

**Cryptography**

User requests to All Day TA's systems are encrypted using Transport Layer Security (TLS) using certificates from an established third party certificate authority. Remote system administration access to All Day TA web and application servers is available through cryptographic network protocols (i.e., SSH) or an encrypted virtual private network (VPN) connection. Data at rest is encrypted using Advanced Encryption Standard (AES) 256 bit.

**Change Management**

A documented Change Management Policy guides all staff members in documenting and implementing application and infrastructure changes. It outlines how changes to the All Day TA are reviewed, deployed, and managed. The policy covers all changes made to the All Day TA software application, regardless of their size, scope, or potential impact.

The Change Management Policy is designed to mitigate the risks of:

- Corrupted or destroyed information
- Degraded or disrupted software application performance
- Productivity loss
- Introduction of software bugs, configuration errors, vulnerabilities, etc.

The ability to implement changes into the production infrastructure is restricted to only those individuals who require the ability to implement changes as part of their responsibilities.

Further AWS CloudTrail is configured to track all changes to the production infrastructure. Customer content and personal information are not used in non-production environments.

#### Software Security Assurance

Secure coding practices are established based on the programming language and development environment used. In-house developed software includes explicit error checking and documented inputs, including for size, data type, and acceptable ranges or formats. Security analysis is performed to verify secure coding practices are followed during change control. Vulnerabilities identified, if any, are tracked to resolution.

#### Asset Management (Hardware and Software)

Assets used in the system are inventoried or tagged to include business descriptions, asset ownership, versions, and other configuration levels, as appropriate, to help ensure assets are classified appropriately, patched, and tracked as part of configuration management. All Day TA uses tagging tools to automatically facilitate the company's hardware and software asset inventory. This helps to ensure a complete and accurate inventory of technology assets with the potential to store or process information is maintained.

#### Vulnerability Management

Vulnerability scanning tools are used to automatically scan systems on the network at least monthly to identify potential vulnerabilities. Automated software update tools are used to help ensure operating systems are running the most recent security updates provided by the software vendor. Vulnerabilities identified are risk-ranked to prioritize the remediation of discovered vulnerabilities.

- User entity is responsible for sending data to All Day TA's software application via a secure connection and/or the data should be encrypted.
- User entity is responsible for notifying All Day TA's software application if they detect or suspect a security incident related to the All Day TA.
- User entity is responsible for reviewing email and other forms of communications from All Day TA, related to changes that may affect All Day TA customers and users, and their security or availability obligations.

## *Monitoring Controls*

All Day TA's management monitors controls to ensure that they are operating as intended and that the controls are modified as conditions change. Monitoring activities are undertaken to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Staff activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, independent evaluations, or a combination of the two.

## *Information and Communication*

All Day TA maintains a company-wide Information Security Policy, supported by detailed standards and training to ensure that employees understand their individual roles and responsibilities regarding security and significant events.

Further, All Day TA also has additional policies and procedures that define access management, change management, and authentication requirements and procedures for critical systems. These policies and procedures are published and made available to internal staff via the company intranet.

Information about the system and services are maintained and made available to users on the company website.

## DC 6: Complementary User Entity Controls

All Day TA's controls were designed with the assumption that certain internal controls would be in place at customer organizations. The application of such internal controls by customer organizations is necessary to achieve certain trust services criteria identified in this report. In addition, there may be control activities that are not identified in this report that would be appropriate for processing of transactions for All Day TA customers.

For customers to rely on the information processed through the All Day TA's software application, each customer is expected to evaluate its own internal controls to ensure appropriate control activities are in place. The following general procedures and controls should be considered. They should not, however, be regarded as a comprehensive list of all controls that should be implemented by customer organizations.

- User entity is responsible for managing their organization's All Day TA's software application

**Endpoint Management**

Endpoint management solutions are in place that include policy enforcement on company issued devices, as well as bring-your-own devices that could connect to or access data within the system boundaries. Policies enforced on endpoints include encryption on devices for data at rest.

To help prevent malware, the following are implemented within the organization:

- Email attachments entering the organization's email gateway are scanned for viruses; and,
- Anti-malware software to continuously monitor and defend each of the organization's workstations and servers.

**Availability**

All Day TA has a documented business continuity plan (BCP) and testing performed against the recovery time objectives (RTOs) and recovery point objectives (RPOs). At least daily backup schedules are maintained to protect sensitive data from loss in the event of a system

failure. Backups are restored at least annually as part of operational activities and are included as part of the BCP test plan.

- Account as well as establishing any customized security solutions or automated processes through the use of setup features
- User entity is responsible for protecting established user IDs and passwords within their organizations.
- User entity is responsible for reviewing customer access to the All Day TA's software application periodically to validate appropriateness of access levels.
- User entity is responsible for approving and creating new user access to the All Day TA's software application.
- User entity is responsible for removing terminated employee access to the All Day TA's software application.
- User entity is responsible for implementing policies and procedures over the types of data that are allowed to be entered into the All Day TA's software application.
- User entity is responsible for establishing, monitoring, and maintaining controls over the security for system-generated outputs and reports from the system.
- User entity is responsible for endpoint protection of workstations used to access the system.
- User entity is responsible for developing their own business continuity and disaster recovery plan

## DC 7: Complementary Subservice Organizations Controls

All Day TA uses subservice organizations in support of its system. All Day TA's controls related to the system cover only a portion of overall internal control for user entities. It is not feasible for the trust services criteria over the All Day TA to be achieved solely by All Day TA. Therefore, user entity controls must be evaluated in conjunction with All Day TA's controls described in Section IV of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

All Day TA periodically reviews the quality of the outsourced operations by various methods including:

| Control Activity Expected to be Implemented by Subservice Organization | Subservice Organization | Applicable Criteria |
|---|---|---|
| Logical access to the underlying network and virtualization management software for the cloud architecture is appropriate. | AWS | CC6.1, CC6.2, CC6.3, CC6.5, CC7.2 |
| Physical access to the data center facility is restricted to authorized personnel. | AWS | CC6.4, CC6.5 |
| Environmental protection, including monitoring and alarming mechanisms, are implemented to address physical security and environmental control requirements. | AWS | CC6.4, A1.2 |
| Business continuity and disaster recovery procedures are developed, reviewed, and tested periodically. | AWS | A1.3 |
| Policies and procedures to document repairs and modifications to the physical components of a facility including, but not limited to, hardware, walls, doors, locks, and other physical security components. | AWS | A1.2 |
| A defined Data Classification Policy specifies classification levels and control requirements in order to meet the company's commitments related to confidentiality. | AWS | C1.1 |
| A defined process is in place to sanitize and destroy hard drives and back up media containing customer data prior to leaving company facilities. | AWS | C1.2 |

## DC 8: Criteria not applicable to the system

All Common Criteria/Security, Confidentiality, and Availability Criteria were applicable to the All Day TA platform system.

## DC 9: Disclosure of Significant changes in last 1 year

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

# SECTION 4

TESTING MATRIX

# TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

**Scope of Testing**
This report on the controls relates to the All Day TA System provided by All Day TA. The scope of the testing was restricted to the All Day TA System and its boundaries as defined in Section 3. AT and F International, Inc. conducted the examination testing over the period February 15, 2025 to August 15, 2025.

**Tests of Operating Effectiveness**
The tests applied to test the operating effectiveness of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that the applicable trust services criteria were achieved during the period. In selecting the tests of controls, AT and F International, Inc. considered various factors including, but not limited to, the following:

- the nature of the control and the frequency with which it operates;
- the control risk mitigated by the control;
- the effectiveness of entity-level controls, especially controls that monitor other controls;
- the degree to which the control relies on the effectiveness of other controls; and
- whether the control is manually performed or automated.

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

| Test Approach | Description |
|---|---|
| Inquiry | Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, emails, web-based conferences, or a combination of the preceding. |
| Observation | Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures. |
| Inspection | Inspected the relevant audit records. This included, but was not limited to, documents, system configurations and settings, or the existence of sampling attributes, such as signatures, approvals, or logged events. In some cases, inspection testing involved tracing events forward to consequent system documentation or processes (e.g.,resolution, detailed documentation, alarms, etc.) or vouching backwards for prerequisite events (e.g., approvals, authorizations, etc.). |
| Re-performance | Re-performed the control to verify the design and / or operation of the control activity as performed if applicable. |

**Sampling**
Consistent with American Institute of Certified Public Accountants (AICPA) authoritative literature, AT and F International, Inc utilizes professional judgment to consider the tolerable deviation rate, the

expected deviation rate, the audit risk, the characteristics of the population, and other factors, in order to determine the number of items to be selected in
a sample for a particular test. AT and F International, Inc, in accordance with AICPA authoritative literature, selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

System-generated population listings were obtained whenever possible to ensure completeness prior to selecting samples. In some instances, full populations were tested in cases including but not limited to, the uniqueness of the event or low overall population size.

**Reliability of Information Provided by the Service Organization**
Observation and inspection procedures were performed related to certain system-generated reports, listings, and queries to assess the accuracy and completeness (reliability) of the information used in the performance of our testing of the controls.

**Test Results**
The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase “No exceptions noted.” in the test result column of the Testing Matrices. Any phrase other than the aforementioned, constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the operating effectiveness
of the control activity. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors. Control considerations that should be implemented by subservice organizations, in order to complement the control activities and achieve the service commitments and system requirements, are presented in the “Subservice Organizations” section within Section 3.

# SECURITY CATEGORY

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **Control Environment** | | | |
| **CC1.1** COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values. | | | |
| CC1.1 | All Day TA Management has approved security policies, and all employees accept these procedures when hired. Management also ensures that security policies are accessible to all employees and contractors. | Inspected the organization's approved security policies, inspected a sample of new-hire records for evidence of employee acknowledgment, and verified that the policies are published and accessible to all employees and contractors. | No exceptions noted. |
| CC1.1 | All Day TA has policies and procedures in place to establish acceptable use of information assets approved by management, posted on the company wiki, and accessible to all employees. All employees must accept the Acceptable Use Policy upon hire. | Inspected the organization's Acceptable Use Policy to verify it was approved by management, confirmed it was posted on the company wiki and accessible to all employees, and reviewed a sample of new hire records to ensure acceptance upon hire. | No exceptions noted. |
| CC1.1 | All Day TA requires its contractors to read and accept the Code of Conduct, read and accept the Acceptable Use Policy, and pass a background check. | Inspected personnel records to verify completion of background checks and reviewed acknowledgments to confirm that individuals read and accepted the Code of Conduct and Acceptable Use Policy. | No exceptions noted. |
| CC1.1 | All Day TA has a formal Code of Conduct approved by management and accessible to all employees. All employees must accept the Code of Conduct upon hire. | Inspected the organization's Code of Conduct to verify it was formally approved by management, confirmed it was accessible to employees, and reviewed a sample of new hire records to ensure acceptance upon hire. | No exceptions noted. |
| CC1.1 | All Day TA's new hires are required to pass a background check as a condition of their | Inspected new hire personnel records and hiring documentation to verify that background checks were | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | employment. | conducted and successfully completed as a condition of employment prior to start date. | |
| CC1.1 | All Day TA has established a Data Protection Policy and requires all employees to accept it upon hire. Management monitors employees' acceptance of the policy. | Inspected the organization's Data Protection Policy to verify it was formally established, and reviewed a sample of employee records to confirm acceptance of the policy upon hire. Additionally, inspected evidence that management monitors employee acknowledgments. | No exceptions noted. |
| **CC1.2** COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control. | | | |
| CC1.2 | The company's board members have sufficient expertise to oversee management's ability to design, implement and operate information security controls. The board engages third-party information security experts and consultants as needed. | Inspected board documentation to verify oversight of information security activities, inspected evidence of third-party experts or consultants engaged as needed, and considered professional profiles (e.g., LinkedIn) to confirm board members possessed sufficient expertise. | No exceptions noted. |
| CC1.2 | All Day TA engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high priority findings are tracked to resolution. | Inspected vulnerability scan reports, management review evidence, supporting documentation, and remediation tracking records to verify scans are performed timely, results are thoroughly reviewed, and high-priority findings are resolved. | No exceptions noted. |
| CC1.2 | The company's board of directors or a relevant subcommittee is briefed by senior management at least annually on the state of the company's cybersecurity and privacy risk. The board provides feedback and direction to management as needed. | Inspected Security Committee quarterly meeting minutes to verify that management provided updates on cybersecurity and privacy risks and confirmed that the committee provided feedback and direction as appropriate. | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| CC1.2 | All Day TA has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines. | Inspected documentation identifying the organization's assigned security team, reviewed role descriptions and responsibilities, and confirmed that the team was accountable for the design, implementation, management, and review of security policies, standards, procedures, and guidelines. | No exceptions noted. |
| CC1.2 | Management has established defined roles and responsibilities to oversee implementation of the information security policy across the organization. | Inspected documentation defining roles and responsibilities for oversight of the Information Security Policy and confirmed that management assigned accountability for implementation across the organization. | No exceptions noted. |
| CC1.2 | The company's board of directors meets at least annually and maintains formal meeting minutes. The board includes directors that are independent of the company. | Inspected board meeting minutes to confirm meetings were held at least annually and formally documented. Inspected the composition of the Board to verify that independent directors are included. | No exceptions noted. |
| CC1.2 | Members of the Board of Directors are independent of management. | Inspected the composition of the Board of Directors and reviewed biographical information and role documentation to confirm that members serving on the Board are independent of management. | No exceptions noted. |
| CC1.2 | Management reviews security policies on an annual basis. | Inspected documentation of management's review of security policies to verify that reviews were conducted on an annual basis and confirmed evidence of approval or sign-off. | No exceptions noted. |
| CC1.2 | All Day TA conducts a Risk Assessment at least annually. | Inspected documentation of the organization's risk assessment process and reviewed evidence of the most recent annual risk assessment | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | to confirm that it was conducted in accordance with policy. | |
| CC1.2 | All Day TA engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution. | Inspected evidence of the most recent third-party penetration test of the production environment, reviewed management's documentation of the results, and examined a sample of high-priority findings to confirm they were tracked through remediation to resolution. | No exceptions noted. |
| **CC1.3** COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. | | | |
| CC1.3 | All Day TA reviews its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis. | Inspected the organizational chart and supporting documentation to confirm reporting lines, authorities, and responsibilities are formally reviewed and approved on at least an annual basis. | No exceptions noted. |
| CC1.3 | All Day TA has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines. | Inspected documentation identifying the organization's assigned security team, reviewed role descriptions and responsibilities, and confirmed that the team was accountable for the design, implementation, management, and review of security policies, standards, procedures, and guidelines. | No exceptions noted. |
| **CC1.4** COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. | | | |
| CC1.4 | All Day TA positions have a detailed job description that lists qualifications, such as requisite skills and experience, which candidates must meet in order to be hired by All Day TA. | Inspected a sample of job descriptions to confirm they included detailed qualifications, requisite skills, and experience requirements that candidates must meet before being hired. | No exceptions noted. |
| CC1.4 | All Day TA's new hires and/or internal transfers are required to go through an official recruiting process during | Inspected samples of recruiting and onboarding records, including resumes, and screening documentation, | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | which their qualifications and experience are screened to ensure that they are competent and capable of fulfilling their responsibilities. | to verify that new hires and internal transfers underwent a formal recruiting process to assess qualifications and experience before assuming responsibilities. | |
| CC1.4 | All Day TA requires its contractors to read and accept the Code of Conduct, read and accept the Acceptable Use Policy, and pass a background check. | Inspected personnel records to verify completion of background checks and reviewed acknowledgments to confirm that individuals read and accepted the Code of Conduct and Acceptable Use Policy. | No exceptions noted. |
| CC1.4 | All Day TA evaluates the performance of all employees through a formal, annual performance evaluation. | Inspected documentation of the organization’s performance evaluation process and reviewed evidence of annual performance evaluations to confirm that all employees were assessed in accordance with policy. | No exceptions noted. |
| CC1.4 | All Day TA has a formal Code of Conduct approved by management and accessible to all employees. All employees must accept the Code of Conduct upon hire. | Inspected the organization’s Code of Conduct to verify it was formally approved by management, confirmed it was accessible to employees, and reviewed a sample of new hire records to ensure acceptance upon hire. | No exceptions noted. |
| CC1.4 | All Day TA's new hires are required to pass a background check as a condition of their employment. | Inspected new hire personnel records and hiring documentation to verify that background checks were conducted and successfully completed as a condition of employment prior to start date. | No exceptions noted. |
| CC1.4 | All Day TA has established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with All Day TA's security policies and procedures, including the identification and reporting of incidents. All full-time | Inspected the organization’s privacy and information security training materials to verify they addressed employee obligations, responsibilities, and incident reporting, and reviewed training records to confirm that all full-time employees | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | employees are required to complete the training upon hire and annually thereafter. | completed the training upon hire and annually thereafter. | |
| **CC1.5** COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives. | | | |
| CC1.5 | All Day TA has policies and procedures in place to establish acceptable use of information assets approved by management, posted on the company wiki, and accessible to all employees. All employees must accept the Acceptable Use Policy upon hire. | Inspected the organization's Acceptable Use Policy to verify it was approved by management, confirmed it was posted on the company wiki and accessible to all employees, and reviewed a sample of new hire records to ensure acceptance upon hire. | No exceptions noted. |
| CC1.5 | All Day TA evaluates the performance of all employees through a formal, annual performance evaluation. | Inspected documentation of the organization's performance evaluation process and reviewed evidence of annual performance evaluations to confirm that all employees were assessed in accordance with policy. | No exceptions noted. |
| CC1.5 | All Day TA has a formal Code of Conduct approved by management and accessible to all employees. All employees must accept the Code of Conduct upon hire. | Inspected the organization's Code of Conduct to verify it was formally approved by management, confirmed it was accessible to employees, and reviewed a sample of new hire records to ensure acceptance upon hire. | No exceptions noted. |
| CC1.5 | All Day TA has established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with All Day TA's security policies and procedures, including the identification and reporting of incidents. All full-time employees are required to complete the training upon hire and annually thereafter. | Inspected the organization's privacy and information security training materials to verify they addressed employee obligations, responsibilities, and incident reporting, and reviewed training records to confirm that all full-time employees completed the training upon hire and annually thereafter. | No exceptions noted. |
| **Information and Communication** | | | |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CC2.1** COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control. | | | |
| CC2.1 | All Day TA conducts continuous monitoring of security controls using Socurely, and addresses issues in a timely manner. | Inspected evidence from the organization's continuous monitoring tool (Socurely) to verify that security controls were actively monitored and reviewed documentation showing that identified issues were addressed by management in a timely manner. | No exceptions noted. |
| CC2.1 | All Day TA has an established policy and procedures that governs the use of cryptographic controls. | Inspected the organization's Key Management and Cryptography Policy to verify it documented the use of cryptographic controls and reviewed evidence of management approval of the policy. | No exceptions noted. |
| CC2.1 | All Day TA maintains an accurate architecture diagram to document system boundaries to support the functioning of internal control. | Inspected the organization's architecture diagram to verify that it accurately documented system components and boundaries and confirmed it was maintained to support the functioning of internal controls. | No exceptions noted. |
| CC2.1 | All Day TA Management has approved all policies that detail how customer data may be made accessible and should be handled. These policies are accessible to all employees and contractors. | Inspected management-approved policies governing the handling and accessibility of customer data, and confirmed that the policies were made available to all employees and contractors. | No exceptions noted. |
| CC2.1 | All Day TA has a defined Information Security Policy that covers policies and procedures to support the functioning of internal control. | Inspected the organization's Information Security Policy to verify it included policies and procedures designed to support the functioning of internal controls, and confirmed management approval of the policy. | No exceptions noted. |
| CC2.1 | All Day TA authorizes access to information resources, including data and the | Inspected access control policies and a sample of user access listings to verify that | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | systems that store or process customer data, based on the principle of least privilege. | access to information resources and systems processing customer data is authorized in accordance with the principle of least privilege. | |
| CC2.1 | All Day TA conducts a Risk Assessment at least annually. | Inspected documentation of the organization's risk assessment process and reviewed evidence of the most recent annual risk assessment to confirm that it was conducted in accordance with policy. | No exceptions noted. |
| CC2.1 | All Day TA identifies, inventories and classifies virtualized assets. | Inspected the organization's asset inventory to verify that virtualized assets were identified, recorded, and classified in accordance with management's requirements. | No exceptions noted. |
| CC2.1 | All Day TA performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. | Inspected documentation of the organization's annual control self-assessments to verify they were performed, and reviewed evidence of corrective actions taken to address identified findings. | No exceptions noted. |
| **CC2.2** COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control. | | | |
| CC2.2 | All Day TA has an established Incident Response Policy that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing. | Inspected the organization's Incident Response Policy to verify its documented management responsibilities and procedures for responding to security incidents, and reviewed evidence of annual testing to confirm the plan was exercised. | No exceptions noted. |
| CC2.2 | All Day TA has implemented an Incident Response Policy that includes creating, prioritizing, assigning, and tracking follow-ups to completion. | Inspected the organization's Incident Response Policy to verify it included procedures for creating, prioritizing, assigning, and tracking incidents through resolution, and reviewed a sample of incident tickets to confirm that | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | follow-ups were tracked to completion. | |
| CC2.2 | All Day TA conducts continuous monitoring of security controls using Socurely, and addresses issues in a timely manner. | Inspected evidence from the organization's continuous monitoring tool (Socurely) to verify that security controls were actively monitored and reviewed documentation showing that identified issues were addressed by management in a timely manner. | No exceptions noted. |
| CC2.2 | All Day TA Management has approved security policies, and all employees accept these procedures when hired. Management also ensures that security policies are accessible to all employees and contractors. | Inspected the organization's approved security policies, inspected a sample of new-hire records for evidence of employee acknowledgment, and verified that the policies are published and accessible to all employees and contractors. | No exceptions noted. |
| CC2.2 | All Day TA has policies and procedures in place to establish acceptable use of information assets approved by management, posted on the company wiki, and accessible to all employees. All employees must accept the Acceptable Use Policy upon hire. | Inspected the organization's Acceptable Use Policy to verify it was approved by management, confirmed it was posted on the company wiki and accessible to all employees, and reviewed a sample of new hire records to ensure acceptance upon hire. | No exceptions noted. |
| CC2.2 | All Day TA has a formal Code of Conduct approved by management and accessible to all employees. All employees must accept the Code of Conduct upon hire. | Inspected the organization's Code of Conduct to verify it was formally approved by management, confirmed it was accessible to employees, and reviewed a sample of new hire records to ensure acceptance upon hire. | No exceptions noted. |
| CC2.2 | All Day TA has established a Data Protection Policy and requires all employees to accept it upon hire. Management monitors employees' acceptance of the policy. | Inspected the organization's Data Protection Policy to verify it was formally established, and reviewed a sample of employee records to confirm acceptance of the policy upon hire. Additionally, inspected evidence that management | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | monitors employee acknowledgments. | |
| CC2.2 | All Day TA has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company. | Inspected documentation identifying the incident response team and reviewed incident management records to confirm the team quantified and monitored incidents related to security, availability, processing integrity, and confidentiality. | No exceptions noted. |
| CC2.2 | All Day TA has implemented an Incident Response Policy that includes documenting Lessons Learned and "Root Cause Analysis" after incidents and sharing them with the broader engineering team. | Inspected the organization's incident response documentation to verify that lessons learned and root cause analysis were recorded following an incident exercise, and reviewed evidence that outcomes were communicated to relevant engineering teams. | No exceptions noted. |
| CC2.2 | All Day TA provides a process to employees for reporting security, confidentiality, integrity, and availability features, incidents, and concerns, and other complaints to company management. | Inspected policies and procedures outlining the reporting channels available to employees to confirm that security, confidentiality, integrity, and availability concerns can be escalated to management.<br>Also, Inspected evidence of reporting mechanisms via. helpdesk portal, and email alias to verify employees are provided with a process for reporting incidents and concerns to management. | No exceptions noted. |
| CC2.2 | All Day TA has established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with All Day TA's security policies and procedures, including the identification and reporting of incidents. All full-time employees are required to complete the training upon hire and annually thereafter. | Inspected the organization's privacy and information security training materials to verify they addressed employee obligations, responsibilities, and incident reporting, and reviewed training records to confirm that all full-time employees completed the training upon hire and annually thereafter. | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | | |
| CC2.2 | The security team communicates important information security events to company management in a timely manner. | Inspected documentation of the organization's BCP/DR tabletop exercise to verify it was conducted in accordance with the Business Continuity and Disaster Recovery Plan, and reviewed records of participants, scenarios, and outcomes to confirm results were documented and approved by management. | No exceptions noted. |
| **CC2.3** COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control. | | | |
| CC2.3 | All Day TA maintains a Terms of Service that is available to all external users and internal employees, and the terms detail the company's security and availability commitments regarding the systems. Client Agreements or Master Service Agreements are in place for when the Terms of Service may not apply. | Inspected the organization's Legal Documents page on the website to verify it included security and availability commitments and confirmed that it was accessible to both external users and internal employees. Additionally, inspected client agreements and master service agreements to confirm they were established where the Terms of Service did not apply. | No exceptions noted. |
| CC2.3 | All Day TA has an established Incident Response Policy that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing. | Inspected the organization's Incident Response Policy to verify its documented management responsibilities and procedures for responding to security incidents, and reviewed evidence of annual testing to confirm the plan was exercised. | No exceptions noted. |
| CC2.3 | All Day TA has implemented an Incident Response Policy that includes creating, prioritizing, assigning, and tracking follow-ups to completion. | Inspected the organization's Incident Response Policy to verify it included procedures for creating, prioritizing, assigning, and tracking incidents through resolution, and reviewed a sample of incident tickets to confirm that follow-ups were tracked to completion. | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| CC2.3 | All Day TA tracks security deficiencies through internal tools and closes them within an SLA that management has pre-specified. | Inspected internal tracking tool records and management reports to confirm security deficiencies are logged and tracked. Inspected sample deficiencies to verify that they were remediated and closed within the SLA timeframes defined by management. | No exceptions noted. |
| CC2.3 | All Day TA's security commitments are communicated to external users, as appropriate. | Inspected customer-facing documentation, such as the organization's website and security or privacy policies, to verify that security commitments were communicated to external users, as appropriate. | No exceptions noted. |
| CC2.3 | All Day TA provides a process to external users for reporting security, confidentiality, integrity, and availability failures, incidents, concerns, and other complaints. | Inspected the organization's website to verify that external users were provided with a means to report security, confidentiality, integrity, and availability concerns (via the Contact Us page), and reviewed internal procedures to confirm that reported issues were tracked and addressed by management. | No exceptions noted. |
| CC2.3 | All Day TA communicates system changes to customers that may affect security, availability, processing integrity, or confidentiality. | Inspected the organization's published release notes to verify that system changes with potential impact on security, availability, processing integrity, or confidentiality were communicated to customers. | No exceptions noted. |
| CC2.3 | All Day TA has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company. | Inspected documentation identifying the incident response team and reviewed incident management records to confirm the team quantified and monitored incidents related to security, availability, processing integrity, and confidentiality. | No exceptions noted. |
| CC2.3 | All Day TA has implemented an Incident Response Policy | Inspected the organization's incident response | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | that includes documenting Lessons Learned and "Root Cause Analysis" after incidents and sharing them with the broader engineering team. | documentation to verify that lessons learned and root cause analysis were recorded following an incident exercise, and reviewed evidence that outcomes were communicated to relevant engineering teams. | |
| CC2.3 | All Day TA maintains a Privacy Policy that is available to all external users and internal employees, and it details the company's confidentiality and privacy commitments. | Inspected the organization's Privacy Policy to verify that it documented confidentiality and privacy commitments, and confirmed that the policy was made available to both external users and internal employees. | No exceptions noted. |
| CC2.3 | All Day TA maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually. | Inspected the organization's vendor directory to verify that it included key vendors and their compliance reports, and reviewed evidence of annual reviews of critical vendor compliance reports performed by management. | No exceptions noted. |
| **Risk Assessment** | | | |
| **CC3.1** COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. | | | |
| CC3.1 | All Day TA has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances. | Inspected the organization's documented risk management process to verify it specified risk tolerances and outlined procedures for evaluating risks, and reviewed evidence of risk assessments performed to confirm the process was applied. | No exceptions noted. |
| CC3.1 | All Day TA engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high priority findings are tracked to resolution. | Inspected vulnerability scan reports, management review evidence, supporting documentation, and remediation tracking records to verify scans are performed timely, results are thoroughly reviewed, and high-priority findings are resolved. | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| CC3.1 | All Day TA conducts a Risk Assessment at least annually. | Inspected documentation of the organization's risk assessment process and reviewed evidence of the most recent annual risk assessment to confirm that it was conducted in accordance with policy. | No exceptions noted. |
| CC3.1 | All Day TA engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution. | Inspected evidence of the most recent third-party penetration test of the production environment, reviewed management's documentation of the results, and examined a sample of high-priority findings to confirm they were tracked through remediation to resolution. | No exceptions noted. |
| **CC3.2** COSO Principle 7: 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. | | | |
| CC3.2 | All Day TA has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances. | Inspected the organization's documented risk management process to verify it specified risk tolerances and outlined procedures for evaluating risks, and reviewed evidence of risk assessments performed to confirm the process was applied. | No exceptions noted. |
| CC3.2 | All Day TA engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high priority findings are tracked to resolution. | Inspected vulnerability scan reports, management review evidence, supporting documentation, and remediation tracking records to verify scans are performed timely, results are thoroughly reviewed, and high-priority findings are resolved. | No exceptions noted. |
| CC3.2 | All Day TA's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities, including fraud. | Inspected the organization's Risk Mitigation Report to verify that management prepared a remediation plan addressing findings from risk assessments, including fraud-related risks, and reviewed evidence that | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | responsibilities, timelines, and treatment actions were documented to ensure risks were formally managed. | |
| CC3.2 | All Day TA conducts a Risk Assessment at least annually. | Inspected documentation of the organization's risk assessment process and reviewed evidence of the most recent annual risk assessment to confirm that it was conducted in accordance with policy. | No exceptions noted. |
| CC3.2 | All Day TA maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually. | Inspected the organization's vendor directory to verify that it included key vendors and their compliance reports, and reviewed evidence of annual reviews of critical vendor compliance reports performed by management. | No exceptions noted. |
| **CC3.3** COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives. | | | |
| CC3.3 | All Day TA's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities, including fraud. | Inspected the organization's Risk Mitigation Report to verify that management prepared a remediation plan addressing findings from risk assessments, including fraud-related risks, and reviewed evidence that responsibilities, timelines, and treatment actions were documented to ensure risks were formally managed. | No exceptions noted. |
| CC3.3 | All Day TA conducts a Risk Assessment at least annually. | Inspected documentation of the organization's risk assessment process and reviewed evidence of the most recent annual risk assessment to confirm that it was conducted in accordance with policy. | No exceptions noted. |
| **CC3.4** COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control. | | | |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| CC3.4 | All Day TA reviews its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis. | Inspected the organizational chart and supporting documentation to confirm reporting lines, authorities, and responsibilities are formally reviewed and approved on at least an annual basis. | No exceptions noted. |
| CC3.4 | All Day TA engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high priority findings are tracked to resolution. | Inspected vulnerability scan reports, management review evidence, supporting documentation, and remediation tracking records to verify scans are performed timely, results are thoroughly reviewed, and high-priority findings are resolved. | No exceptions noted. |
| CC3.4 | All Day TA conducts a Risk Assessment at least annually. | Inspected documentation of the organization's risk assessment process and reviewed evidence of the most recent annual risk assessment to confirm that it was conducted in accordance with policy. | No exceptions noted. |
| CC3.4 | All Day TA engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution. | Inspected evidence of the most recent third-party penetration test of the production environment, reviewed management's documentation of the results, and examined a sample of high-priority findings to confirm they were tracked through remediation to resolution. | No exceptions noted. |
| **Monitoring Activities** | | | |
| **CC4.1** COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. | | | |
| CC4.1 | All Day TA engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high priority findings are tracked to resolution. | Inspected vulnerability scan reports, management review evidence, supporting documentation, and remediation tracking records to verify scans are performed timely, results are thoroughly | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | reviewed, and high-priority findings are resolved. | |
| CC4.1 | All Day TA has a defined System Access Control Policy that requires access to new hires has to be provisioned by management. | Inspected the System Access Control Policy to confirm it requires management authorization for provisioning access to new hires. Inspected a sample of new hire access provisioning records to verify that access was approved and provisioned by management. | No exceptions noted. |
| CC4.1 | All Day TA performs annual access control reviews. | Inspected documentation of the organization's access control review process and reviewed evidence of the most recent annual access review to confirm it was performed by management. | No exceptions noted. |
| CC4.1 | All Day TA conducts a Risk Assessment at least annually. | Inspected documentation of the organization's risk assessment process and reviewed evidence of the most recent annual risk assessment to confirm that it was conducted in accordance with policy. | No exceptions noted. |
| CC4.1 | All Day TA engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution. | Inspected evidence of the most recent third-party penetration test of the production environment, reviewed management's documentation of the results, and examined a sample of high-priority findings to confirm they were tracked through remediation to resolution. | No exceptions noted. |
| **CC4.2** COSO Principle 17: 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. | | | |
| CC4.2 | All Day TA has an established Incident Response Policy that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information | Inspected the organization's Incident Response Policy to verify its documented management responsibilities and procedures for responding to security incidents, and reviewed evidence of annual | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | security incidents and annual testing. | testing to confirm the plan was exercised. | |
| CC4.2 | All Day TA has implemented an Incident Response Policy that includes creating, prioritizing, assigning, and tracking follow-ups to completion. | Inspected the organization's Incident Response Policy to verify it included procedures for creating, prioritizing, assigning, and tracking incidents through resolution, and reviewed a sample of incident tickets to confirm that follow-ups were tracked to completion. | No exceptions noted. |
| CC4.2 | All Day TA engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high priority findings are tracked to resolution. | Inspected vulnerability scan reports, management review evidence, supporting documentation, and remediation tracking records to verify scans are performed timely, results are thoroughly reviewed, and high-priority findings are resolved. | No exceptions noted. |
| CC4.2 | All Day TA has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines. | Inspected documentation identifying the organization's assigned security team, reviewed role descriptions and responsibilities, and confirmed that the team was accountable for the design, implementation, management, and review of security policies, standards, procedures, and guidelines. | No exceptions noted. |
| CC4.2 | All Day TA's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities, including fraud. | Inspected the organization's Risk Mitigation Report to verify that management prepared a remediation plan addressing findings from risk assessments, including fraud-related risks, and reviewed evidence that responsibilities, timelines, and treatment actions were documented to ensure risks were formally managed. | No exceptions noted. |
| CC4.2 | All Day TA conducts a Risk Assessment at least annually. | Inspected documentation of the organization's risk assessment process and reviewed evidence of the most | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | recent annual risk assessment to confirm that it was conducted in accordance with policy. | |
| CC4.2 | All Day TA has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company. | Inspected documentation identifying the incident response team and reviewed incident management records to confirm the team quantified and monitored incidents related to security, availability, processing integrity, and confidentiality. | No exceptions noted. |
| CC4.2 | All Day TA has implemented an Incident Response Policy that includes documenting Lessons Learned and "Root Cause Analysis" after incidents and sharing them with the broader engineering team. | Inspected the organization's incident response documentation to verify that lessons learned and root cause analysis were recorded following an incident exercise, and reviewed evidence that outcomes were communicated to relevant engineering teams. | No exceptions noted. |
| CC4.2 | All Day TA engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution. | Inspected evidence of the most recent third-party penetration test of the production environment, reviewed management's documentation of the results, and examined a sample of high-priority findings to confirm they were tracked through remediation to resolution. | No exceptions noted. |
| **Control Activities** | | | |
| **CC5.1** COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. | | | |
| CC5.1 | All Day TA has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances. | Inspected the organization's documented risk management process to verify it specified risk tolerances and outlined procedures for evaluating risks, and reviewed evidence of risk assessments performed to confirm the process was applied. | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| CC5.1 | All Day TA conducts continuous monitoring of security controls using Socurely, and addresses issues in a timely manner. | Inspected evidence from the organization's continuous monitoring tool (Socurely) to verify that security controls were actively monitored and reviewed documentation showing that identified issues were addressed by management in a timely manner. | No exceptions noted. |
| CC5.1 | All Day TA reviews its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis. | Inspected the organizational chart and supporting documentation to confirm reporting lines, authorities, and responsibilities are formally reviewed and approved on at least an annual basis. | No exceptions noted. |
| CC5.1 | All Day TA engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high priority findings are tracked to resolution. | Inspected vulnerability scan reports, management review evidence, supporting documentation, and remediation tracking records to verify scans are performed timely, results are thoroughly reviewed, and high-priority findings are resolved. | No exceptions noted. |
| CC5.1 | All Day TA has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines. | Inspected documentation identifying the organization's assigned security team, reviewed role descriptions and responsibilities, and confirmed that the team was accountable for the design, implementation, management, and review of security policies, standards, procedures, and guidelines. | No exceptions noted. |
| CC5.1 | All Day TA's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities, including fraud. | Inspected the organization's Risk Mitigation Report to verify that management prepared a remediation plan addressing findings from risk assessments, including fraud-related risks, and reviewed evidence that responsibilities, timelines, and treatment actions were documented to ensure risks were formally managed. | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | | |
| CC5.1 | All Day TA conducts a Risk Assessment at least annually. | Inspected documentation of the organization's risk assessment process and reviewed evidence of the most recent annual risk assessment to confirm that it was conducted in accordance with policy. | No exceptions noted. |
| CC5.1 | All Day TA engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution. | Inspected evidence of the most recent third-party penetration test of the production environment, reviewed management's documentation of the results, and examined a sample of high-priority findings to confirm they were tracked through remediation to resolution. | No exceptions noted. |
| **CC5.2** COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives. | | | |
| CC5.2 | All Day TA conducts continuous monitoring of security controls using Socurely, and addresses issues in a timely manner. | Inspected evidence from the organization's continuous monitoring tool (Socurely) to verify that security controls were actively monitored and reviewed documentation showing that identified issues were addressed by management in a timely manner. | No exceptions noted. |
| CC5.2 | All Day TA Management has approved security policies, and all employees accept these procedures when hired. Management also ensures that security policies are accessible to all employees and contractors. | Inspected the organization's approved security policies, inspected a sample of new-hire records for evidence of employee acknowledgment, and verified that the policies are published and accessible to all employees and contractors. | No exceptions noted. |
| CC5.2 | All Day TA has an established policy and procedures that governs the use of cryptographic controls. | Inspected the organization's Key Management and Cryptography Policy to verify it documented the use of cryptographic controls and reviewed evidence of | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | management approval of the policy. | |
| CC5.2 | All Day TA engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high priority findings are tracked to resolution. | Inspected vulnerability scan reports, management review evidence, supporting documentation, and remediation tracking records to verify scans are performed timely, results are thoroughly reviewed, and high-priority findings are resolved. | No exceptions noted. |
| CC5.2 | All Day TA has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines. | Inspected documentation identifying the organization's assigned security team, reviewed role descriptions and responsibilities, and confirmed that the team was accountable for the design, implementation, management, and review of security policies, standards, procedures, and guidelines. | No exceptions noted. |
| CC5.2 | All Day TA Management has approved all policies that detail how customer data may be made accessible and should be handled. These policies are accessible to all employees and contractors. | Inspected management-approved policies governing the handling and accessibility of customer data, and confirmed that the policies were made available to all employees and contractors. | No exceptions noted. |
| CC5.2 | All Day TA's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities, including fraud. | Inspected the organization's Risk Mitigation Report to verify that management prepared a remediation plan addressing findings from risk assessments, including fraud-related risks, and reviewed evidence that responsibilities, timelines, and treatment actions were documented to ensure risks were formally managed. | No exceptions noted. |
| CC5.2 | All Day TA authorizes access to information resources, including data and the systems that store or process customer data, based on the principle of least privilege. | Inspected access control policies and a sample of user access listings to verify that access to information resources and systems processing customer data is | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | authorized in accordance with the principle of least privilege. | |
| CC5.2 | All Day TA conducts a Risk Assessment at least annually. | Inspected documentation of the organization's risk assessment process and reviewed evidence of the most recent annual risk assessment to confirm that it was conducted in accordance with policy. | No exceptions noted. |
| CC5.2 | All Day TA has established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with All Day TA's security policies and procedures, including the identification and reporting of incidents. All full-time employees are required to complete the training upon hire and annually thereafter. | Inspected the organization's privacy and information security training materials to verify they addressed employee obligations, responsibilities, and incident reporting, and reviewed training records to confirm that all full-time employees completed the training upon hire and annually thereafter. | No exceptions noted. |
| CC5.2 | All Day TA engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution. | Inspected evidence of the most recent third-party penetration test of the production environment, reviewed management's documentation of the results, and examined a sample of high-priority findings to confirm they were tracked through remediation to resolution. | No exceptions noted. |
| **CC5.3** COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action. | | | |
| CC5.3 | All Day TA has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances. | Inspected the organization's documented risk management process to verify it specified risk tolerances and outlined procedures for evaluating risks, and reviewed evidence of risk assessments performed to confirm the process was applied. | No exceptions noted. |
| CC5.3 | All Day TA conducts annual BCP/DR tests and | Inspected documentation of the organization's most recent | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | documents according to the BCDR Plan. | BCP/DR test to verify it was performed in accordance with the Business Continuity and Disaster Recovery Plan and confirmed results were documented by management. | |
| CC5.3 | All Day TA Management has approved security policies, and all employees accept these procedures when hired. Management also ensures that security policies are accessible to all employees and contractors. | Inspected the organization's approved security policies, inspected a sample of new-hire records for evidence of employee acknowledgment, and verified that the policies are published and accessible to all employees and contractors. | No exceptions noted. |
| CC5.3 | All Day TA has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems. | Inspected the organization's Disaster Recovery Plan to verify that it was formally documented and approved by management, and reviewed the plan to confirm that it outlined defined roles, responsibilities, and detailed recovery procedures. | No exceptions noted. |
| CC5.3 | All Day TA has a defined Information Security Policy that covers policies and procedures to support the functioning of internal control. | Inspected the organization's Information Security Policy to verify it included policies and procedures designed to support the functioning of internal controls, and confirmed management approval of the policy. | No exceptions noted. |
| CC5.3 | All Day TA has a formal Code of Conduct approved by management and accessible to all employees. All employees must accept the Code of Conduct upon hire. | Inspected the organization's Code of Conduct to verify it was formally approved by management, confirmed it was accessible to employees, and reviewed a sample of new hire records to ensure acceptance upon hire. | No exceptions noted. |
| CC5.3 | Management reviews security policies on an annual basis. | Inspected documentation of management's review of security policies to verify that reviews were conducted on an annual basis and confirmed evidence of approval or sign-off. | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | | |
| CC5.3 | All Day TA provides a process to employees for reporting security, confidentiality, integrity, and availability features, incidents, and concerns, and other complaints to company management. | Inspected policies and procedures outlining the reporting channels available to employees to confirm that security, confidentiality, integrity, and availability concerns can be escalated to management.<br>Also, Inspected evidence of reporting mechanisms via. helpdesk portal, and email alias to verify employees are provided with a process for reporting incidents and concerns to management. | No exceptions noted. |
| **Logical and Physical Controls** | | | |
| **CC6.1** The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives. | | | |
| CC6.1 | Hardening standards are in place to ensure that newly deployed server instances are appropriately secured. | Enquired with the management regarding the control activity to ascertain that the control operates as described.<br><br>Inspected relevant artefacts to ascertain whether Hardening standards are in place to ensure that newly deployed server instances are appropriately secured. | No exceptions noted. |
| CC6.1 | Access to corporate network, production machines, network devices, and support tools requires a unique ID. | Inspected access control configurations and reviewed a sample of user accounts to verify that access to the corporate network, production systems, network devices, and support tools is restricted through the use of unique user IDs. | No exceptions noted. |
| CC6.1 | All Day TA stores customer data in databases that is encrypted at rest. | Inspected database configuration settings and encryption status reports to confirm that customer data is encrypted at rest. Inspected key management | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | configurations such as KMS settings and key rotation policies to verify encryption is properly implemented and managed. | |
| CC6.1 | Username and password (password standard implemented) or SSO required to authenticate into application, MFA optional for external users, and MFA required for employee users. | Inspected application authentication settings and documentation to verify that login requires standard credentials or SSO, and that MFA is configured in accordance with company requirements. | No exceptions noted. |
| CC6.1 | All Day TA requires two factor authentication to access sensitive systems and applications in the form of user ID, password, OTP and/or certificate. | Inspected system configurations and authentication settings, and reviewed a sample of user access attempts to determine whether multi-factor authentication was required to access sensitive systems and applications. | No exceptions noted. |
| CC6.1 | Role-based security is in place for internal and external users, including super admin users. | Inspected system access configurations and role definitions to verify that role-based security is implemented for internal, external, and super admin users. Reviewed a sample of user accounts to confirm that access was provisioned in accordance with assigned roles. | No exceptions noted. |
| CC6.1 | All Day TA has an established key management process in place to support the organization's use of cryptographic techniques. | Inspected key management policies, procedures, and system settings to verify that cryptographic keys are properly generated, stored, rotated, and retired in line with organizational requirements. | No exceptions noted. |
| CC6.1 | All Day TA ensures that a password manager is installed on all company-issued laptops. | Inspected system configuration and deployment records to verify that a password manager was installed on all company-issued laptops. | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| CC6.1 | All Day TA uses a version control system to manage source code, documentation, release labeling, and other change management tasks. Access to the system must be approved by a system admin. | Inspected version control system settings and access records to verify that code and documentation changes are managed through the system and access is granted only with appropriate approval. | No exceptions noted. |
| CC6.1 | All Day TA maintains an accurate network diagram that is accessible to the engineering team and is reviewed by management on an annual basis. | Inspected the organization's network diagram to verify it accurately reflected the current environment, confirmed it was accessible to the engineering team, and reviewed evidence of annual management review. | No exceptions noted. |
| CC6.1 | All Day TA identifies, inventories and classifies virtualized assets. | Inspected the organization's asset inventory to verify that virtualized assets were identified, recorded, and classified in accordance with management's requirements. | No exceptions noted. |
| CC6.1 | Appropriate levels of access to infrastructure and code review tools are granted to new employees within one week of their start date. | Inspected a sample of user access records for new employees to confirm appropriate access to infrastructure and code review tools was provisioned within one week of their start date. | No exceptions noted. |
| CC6.1 | All Day TA has established formal guidelines for passwords to govern the management and use of authentication mechanisms. | Inspected the company's password policy and related documentation to confirm formal guidelines are established governing password complexity, expiration, and the use of authentication mechanisms. | No exceptions noted. |
| CC6.1 | All Day TA ensures that company-issued laptops have encrypted hard-disks. | Inspected system configuration records to verify that company-issued laptops had hard-disk encryption enabled in accordance with the organization's requirements. | No exceptions noted. |
| **CC6.2** Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. | | | |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized. | | | |
| CC6.2 | Access to corporate network, production machines, network devices, and support tools requires a unique ID. | Inspected access control configurations and reviewed a sample of user accounts to verify that access to the corporate network, production systems, network devices, and support tools is restricted through the use of unique user IDs. | No exceptions noted. |
| CC6.2 | A termination checklist is used to ensure that system access, including physical access, for terminated employees has been removed within one specified time | Inspected the organization's termination checklist and related procedures to verify that a process exists to remove system and physical access upon employee termination. Noted that no terminations occurred during the period. | No exceptions noted. |
| CC6.2 | All Day TA has a defined System Access Control Policy that requires access to new hires has to be provisioned by management. | Inspected the System Access Control Policy to confirm it requires management authorization for provisioning access to new hires. Inspected a sample of new hire access provisioning records to verify that access was approved and provisioned by management. | No exceptions noted. |
| CC6.2 | All Day TA performs annual access control reviews. | Inspected documentation of the organization's access control review process and reviewed evidence of the most recent annual access review to confirm it was performed by management. | No exceptions noted. |
| CC6.2 | External users must accept the Terms of Service prior to their account being created. | Inspected account creation procedures to verify that external users are required to accept the Terms of Service prior to account activation. Examined system-generated evidence to confirm that acceptance was captured for new user accounts. | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| CC6.2 | Access to infrastructure and code review tools is removed from terminated employees within one business day. | Inspected the organization's offboarding procedures to verify that access to infrastructure and code review tools is required to be removed within one business day of termination.<br>Noted that no employee terminations occurred during the period. | No exceptions noted. |
| CC6.2 | Appropriate levels of access to infrastructure and code review tools are granted to new employees within one week of their start date. | Inspected a sample of user access records for new employees to confirm appropriate access to infrastructure and code review tools was provisioned within one week of their start date. | No exceptions noted. |
| **CC6.3** The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives. | | | |
| CC6.3 | Access to corporate network, production machines, network devices, and support tools requires a unique ID. | Inspected access control configurations and reviewed a sample of user accounts to verify that access to the corporate network, production systems, network devices, and support tools is restricted through the use of unique user IDs. | No exceptions noted. |
| CC6.3 | A termination checklist is used to ensure that system access, including physical access, for terminated employees has been removed within one specified time | Inspected the organization's termination checklist and related procedures to verify that a process exists to remove system and physical access upon employee termination. Noted that no terminations occurred during the period. | No exceptions noted. |
| CC6.3 | Role-based security is in place for internal and external users, including super admin users. | Inspected system access configurations and role definitions to verify that role-based security is implemented for internal, external, and super admin users. Reviewed a sample of user accounts to confirm that | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | access was provisioned in accordance with assigned roles. | |
| CC6.3 | All Day TA has a defined System Access Control Policy that requires access to new hires has to be provisioned by management. | Inspected the System Access Control Policy to confirm it requires management authorization for provisioning access to new hires. Inspected a sample of new hire access provisioning records to verify that access was approved and provisioned by management. | No exceptions noted. |
| CC6.3 | All Day TA performs annual access control reviews. | Inspected documentation of the organization's access control review process and reviewed evidence of the most recent annual access review to confirm it was performed by management. | No exceptions noted. |
| CC6.3 | External users must accept the Terms of Service prior to their account being created. | Inspected account creation procedures to verify that external users are required to accept the Terms of Service prior to account activation. Examined system-generated evidence to confirm that acceptance was captured for new user accounts. | No exceptions noted. |
| CC6.3 | Access to infrastructure and code review tools is removed from terminated employees within one business day. | Inspected the organization's offboarding procedures to verify that access to infrastructure and code review tools is required to be removed within one business day of termination.<br>Noted that no employee terminations occurred during the period. | No exceptions noted. |
| CC6.3 | Appropriate levels of access to infrastructure and code review tools are granted to new employees within one week of their start date. | Inspected a sample of user access records for new employees to confirm appropriate access to infrastructure and code review tools was provisioned within one week of their start date. | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CC6.4** The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives. | | | |
| CC6.4 | All Day TA has security policies that have been approved by management and detail how physical access to the company's headquarters is maintained. These policies are accessible to all employees and contractors. | Inspected the organization's security policies to verify that they were approved by management and addressed requirements for maintaining physical access to the company's headquarters. Confirmed that the policies were distributed and accessible to employees and contractors. | No exceptions noted. |
| CC6.4 | A termination checklist is used to ensure that system access, including physical access, for terminated employees has been removed within one specified time | Inspected the organization's termination checklist and related procedures to verify that a process exists to remove system and physical access upon employee termination. Noted that no terminations occurred during the period. | No exceptions noted. |
| CC6.4 | All Day TA performs annual access control reviews. | Inspected documentation of the organization's access control review process and reviewed evidence of the most recent annual access review to confirm it was performed by management. | No exceptions noted. |
| CC6.4 | All Day TA has security policies that have been approved by management and detail how physical security for the company's headquarters is maintained. These policies are accessible to all employees and contractors. | Inspected the organization's security policies to verify that they were approved by management and included requirements for maintaining physical security at the company's headquarters. Confirmed that the policies were made available to employees and contractors through the organization's designated communication channels. | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| CC6.4 | All Day TA maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually. | Inspected the organization's vendor directory to verify that it included key vendors and their compliance reports, and reviewed evidence of annual reviews of critical vendor compliance reports performed by management. | No exceptions noted. |
| **CC6.5** The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives. | | | |
| CC6.5 | A termination checklist is used to ensure that system access, including physical access, for terminated employees has been removed within one specified time | Inspected the organization's termination checklist and related procedures to verify that a process exists to remove system and physical access upon employee termination. Noted that no terminations occurred during the period. | No exceptions noted. |
| CC6.5 | All Day TA has formal policies and procedures in place to guide personnel in the disposal of hardware containing sensitive data. | Inspected the organization's policies and procedures to verify that they included requirements for the secure disposal of hardware containing sensitive data. Noted that no hardware disposals occurred during the period. | No exceptions noted. |
| **CC6.6** The entity implements logical access security measures to protect against threats from sources outside its system boundaries. | | | |
| CC6.6 | All Day TA ensures that all connections to its web application from its users are encrypted. | Inspected web application configuration settings and observed connections to confirm that all user traffic is encrypted in transit using HTTPS/TLS. | No exceptions noted. |
| CC6.6 | Username and password (password standard implemented) or SSO required to authenticate into application, MFA optional for external users, and MFA required for employee users. | Inspected application authentication settings and documentation to verify that login requires standard credentials or SSO, and that MFA is configured in accordance with company requirements. | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| CC6.6 | All Day TA requires two factor authentication to access sensitive systems and applications in the form of user ID, password, OTP and/or certificate. | Inspected system configurations and authentication settings, and reviewed a sample of user access attempts to determine whether multi-factor authentication was required to access sensitive systems and applications. | No exceptions noted. |
| CC6.6 | No public SSH is allowed. | Inspected infrastructure network and server configurations to confirm that public SSH access is disabled.<br><br>Also, Inspected firewall and security group settings to verify only authorized connections are permitted. | No exceptions noted. |
| CC6.6 | All Day TA uses configurations that ensure only approved networking ports and protocols are implemented, including firewalls. | Inspected firewall and network configuration settings to confirm that only approved networking ports and protocols are enabled, and unapproved traffic is restricted. | No exceptions noted. |
| CC6.6 | WAF in place to protect All Day TA's application from outside threats. | Inspected WAF configuration and monitoring dashboards to confirm that the web application is protected from outside threats. Inspected sample WAF alerts or logs to verify the control is operational. | No exceptions noted. |
| CC6.6 | Read/Write access to cloud data storage is configured to restrict public access. | Inspected cloud storage configuration settings to confirm that read/write access is restricted and public access is disabled. Inspected access logs to verify compliance with access restrictions. | No exceptions noted. |
| CC6.6 | All Day TA maintains an accurate network diagram that is accessible to the engineering team and is reviewed by management on an annual basis. | Inspected the organization’s network diagram to verify it accurately reflected the current environment, confirmed it was accessible to the engineering team, and reviewed evidence of annual management review. | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | | |
| CC6.6 | All Day TA automatically logs users out after a predefined inactivity interval and/or closure of the internet browser, and requires users to reauthenticate | Inspected application session configuration settings and observed user session behavior to confirm that users are automatically logged out after a predefined inactivity interval or upon browser closure, and are required to reauthenticate to regain access. | No exceptions noted. |
| CC6.6 | All Day TA has established formal guidelines for passwords to govern the management and use of authentication mechanisms. | Inspected the company's password policy and related documentation to confirm formal guidelines are established governing password complexity, expiration, and the use of authentication mechanisms. | No exceptions noted. |
| CC6.6 | All Day TA ensures that all company-issued computers use a screensaver lock with a timeout of no more than 15 minutes. | Inspected endpoint configuration settings and screenshots to confirm that company-issued computers are configured with a screensaver lock set to activate after no more than 15 minutes of inactivity. | No exceptions noted. |
| **CC6.7** The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives. | | | |
| CC6.7 | All Day TA ensures that all connections to its web application from its users are encrypted. | Inspected web application configuration settings and observed connections to confirm that all user traffic is encrypted in transit using HTTPS/TLS. | No exceptions noted. |
| CC6.7 | All Day TA stores customer data in databases that is encrypted at rest. | Inspected database configuration settings and encryption status reports to confirm that customer data is encrypted at rest. Inspected key management configurations such as KMS settings and key rotation policies to verify encryption is properly implemented and managed. | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | | |
| CC6.7 | No public SSH is allowed. | Inspected infrastructure network and server configurations to confirm that public SSH access is disabled.<br><br>Also, Inspected firewall and security group settings to verify only authorized connections are permitted. | No exceptions noted. |
| CC6.7 | All Day TA's customer data is segregated from the data of other customers | Inspected the system's "Manage Organizations" interface displaying unique organization IDs and names to confirm that customer accounts are logically segregated within the platform, ensuring that each customer's data is separated from other customers' data. | No exceptions noted. |
| CC6.7 | All Day TA uses encryption to protect user authentication and admin sessions of the internal admin tool transmitted over the Internet. | Inspected configuration settings and observed the internal admin tool login session to confirm encryption (e.g., HTTPS/TLS) is enforced to protect user authentication and administrative sessions transmitted over the Internet. | No exceptions noted. |
| CC6.7 | All Day TA ensures that company-issued laptops have encrypted hard-disks. | Inspected system configuration records to verify that company-issued laptops had hard-disk encryption enabled in accordance with the organization's requirements. | No exceptions noted. |
| **CC6.8** The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives. | | | |
| CC6.8 | All Day TA has infrastructure logging configured to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically created, sent to appropriate personnel and resolved, as necessary. | Inspected infrastructure logging configurations and monitoring dashboards to confirm that logs are generated for web traffic and suspicious activity. Inspected sample alert records and incident tickets to verify that anomalous traffic triggers alerts, which are sent to | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | appropriate personnel and tracked through resolution. | |
| CC6.8 | All Day TA ensures that virtual machine OS patches are applied monthly. | Inspected system patch management policy and evidence of recent patching activities via patch logs, reports to confirm that virtual machine operating system patches are applied on a monthly basis. | No exceptions noted. |
| CC6.8 | All Day TA's workstations operating system (OS) security patches are applied automatically. | Inspected workstation configuration settings and patch management reports to confirm that OS security patches are applied automatically. | No exceptions noted. |
| **System Operations** | | | |
| **CC7.1** To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities. | | | |
| CC7.1 | All Day TA has infrastructure logging configured to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically created, sent to appropriate personnel and resolved, as necessary. | Inspected infrastructure logging configurations and monitoring dashboards to confirm that logs are generated for web traffic and suspicious activity. Inspected sample alert records and incident tickets to verify that anomalous traffic triggers alerts, which are sent to appropriate personnel and tracked through resolution. | No exceptions noted. |
| CC7.1 | All Day TA conducts continuous monitoring of security controls using Socurely, and addresses issues in a timely manner. | Inspected evidence from the organization's continuous monitoring tool (Socurely) to verify that security controls were actively monitored and reviewed documentation showing that identified issues were addressed by management in a timely manner. | No exceptions noted. |
| CC7.1 | When All Day TA's application code changes, code reviews and tests are | Inspected code repository records and pull request histories to confirm that code | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | performed by someone other than the person who made the code change. | changes are reviewed and tested by an individual other than the developer who made the change. | |
| CC7.1 | All Day TA engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high priority findings are tracked to resolution. | Inspected vulnerability scan reports, management review evidence, supporting documentation, and remediation tracking records to verify scans are performed timely, results are thoroughly reviewed, and high-priority findings are resolved. | No exceptions noted. |
| CC7.1 | All Day TA uses a version control system to manage source code, documentation, release labeling, and other change management tasks. Access to the system must be approved by a system admin. | Inspected version control system settings and access records to verify that code and documentation changes are managed through the system and access is granted only with appropriate approval. | No exceptions noted. |
| CC7.1 | All Day TA engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution. | Inspected evidence of the most recent third-party penetration test of the production environment, reviewed management's documentation of the results, and examined a sample of high-priority findings to confirm they were tracked through remediation to resolution. | No exceptions noted. |
| **CC7.2** The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events. | | | |
| CC7.2 | All Day TA uses logging software that sends alerts to appropriate personnel. Corrective actions are performed, as necessary, in a timely manner. | Inspected logging configurations and sample alerts to verify that notifications are sent to appropriate personnel and corrective actions are taken in a timely manner. | No exceptions noted. |
| CC7.2 | All Day TA has infrastructure logging configured to monitor web traffic and suspicious activity. When anomalous | Inspected infrastructure logging configurations and monitoring dashboards to confirm that logs are | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | traffic activity is identified, alerts are automatically created, sent to appropriate personnel and resolved, as necessary. | generated for web traffic and suspicious activity. Inspected sample alert records and incident tickets to verify that anomalous traffic triggers alerts, which are sent to appropriate personnel and tracked through resolution. | |
| CC7.2 | All Day TA engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high priority findings are tracked to resolution. | Inspected vulnerability scan reports, management review evidence, supporting documentation, and remediation tracking records to verify scans are performed timely, results are thoroughly reviewed, and high-priority findings are resolved. | No exceptions noted. |
| CC7.2 | All Day TA does not use Root Account on Infrastructure provider | Inspected infrastructure provider account settings and access management configurations to confirm that the root account is not used for day-to-day operations. Inspected evidence of role-based access controls to verify that administrative access is granted through designated user accounts instead of the root account. | No exceptions noted. |
| CC7.2 | All Day TA uses a system that collects and stores server logs in a central location. The system can be queried in an ad hoc fashion by authorized users. | Inspected the centralized logging system configuration (AWS CloudWatch log groups) to confirm that server logs are collected and stored in a central location. Inspected access settings and queried log data to verify that authorized users can perform ad hoc queries. | No exceptions noted. |
| CC7.2 | All Day TA tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource. | Inspected tracking tool records and supporting evidence to verify that security deficiencies are logged, prioritized by severity, and independently reviewed. | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CC7.3** The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures. | | | |
| CC7.3 | All Day TA has an established Incident Response Policy that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing. | Inspected the organization's Incident Response Policy to verify its documented management responsibilities and procedures for responding to security incidents, and reviewed evidence of annual testing to confirm the plan was exercised. | No exceptions noted. |
| CC7.3 | All Day TA has implemented an Incident Response Policy that includes creating, prioritizing, assigning, and tracking follow-ups to completion. | Inspected the organization's Incident Response Policy to verify it included procedures for creating, prioritizing, assigning, and tracking incidents through resolution, and reviewed a sample of incident tickets to confirm that follow-ups were tracked to completion. | No exceptions noted. |
| CC7.3 | All Day TA tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource. | Inspected tracking tool records and supporting evidence to verify that security deficiencies are logged, prioritized by severity, and independently reviewed. | No exceptions noted. |
| CC7.3 | All Day TA has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company. | Inspected documentation identifying the incident response team and reviewed incident management records to confirm the team quantified and monitored incidents related to security, availability, processing integrity, and confidentiality. | No exceptions noted. |
| CC7.3 | All Day TA has implemented an Incident Response Policy that includes documenting Lessons Learned and "Root Cause Analysis" after incidents and sharing them with the broader engineering team. | Inspected the organization's incident response documentation to verify that lessons learned and root cause analysis were recorded following an incident exercise, and reviewed evidence that outcomes were communicated to relevant engineering teams. | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| CC7.3 | The security team communicates important information security events to company management in a timely manner. | Inspected documentation of the organization's BCP/DR tabletop exercise to verify it was conducted in accordance with the Business Continuity and Disaster Recovery Plan, and reviewed records of participants, scenarios, and outcomes to confirm results were documented and approved by management. | No exceptions noted. |
| **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. | | | |
| CC7.4 | All Day TA has an established Incident Response Policy that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing. | Inspected the organization's Incident Response Policy to verify its documented management responsibilities and procedures for responding to security incidents, and reviewed evidence of annual testing to confirm the plan was exercised. | No exceptions noted. |
| CC7.4 | All Day TA has implemented an Incident Response Policy that includes creating, prioritizing, assigning, and tracking follow-ups to completion. | Inspected the organization's Incident Response Policy to verify it included procedures for creating, prioritizing, assigning, and tracking incidents through resolution, and reviewed a sample of incident tickets to confirm that follow-ups were tracked to completion. | No exceptions noted. |
| CC7.4 | All Day TA tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource. | Inspected tracking tool records and supporting evidence to verify that security deficiencies are logged, prioritized by severity, and independently reviewed. | No exceptions noted. |
| CC7.4 | All Day TA has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company. | Inspected documentation identifying the incident response team and reviewed incident management records to confirm the team quantified and monitored incidents related to security, availability, | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | processing integrity, and confidentiality. | |
| CC7.4 | All Day TA has implemented an Incident Response Policy that includes documenting Lessons Learned and "Root Cause Analysis" after incidents and sharing them with the broader engineering team. | Inspected the organization's incident response documentation to verify that lessons learned and root cause analysis were recorded following an incident exercise, and reviewed evidence that outcomes were communicated to relevant engineering teams. | No exceptions noted. |
| **CC7.5** The entity identifies, develops, and implements activities to recover from identified security incidents. | | | |
| CC7.5 | All Day TA has an established Incident Response Policy that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing. | Inspected the organization's Incident Response Policy to verify its documented management responsibilities and procedures for responding to security incidents, and reviewed evidence of annual testing to confirm the plan was exercised. | No exceptions noted. |
| CC7.5 | All Day TA has implemented an Incident Response Policy that includes creating, prioritizing, assigning, and tracking follow-ups to completion. | Inspected the organization's Incident Response Policy to verify it included procedures for creating, prioritizing, assigning, and tracking incidents through resolution, and reviewed a sample of incident tickets to confirm that follow-ups were tracked to completion. | No exceptions noted. |
| CC7.5 | All Day TA performs backups daily and retains them in accordance with a predefined schedule in the Backup Policy. | Inspected the Backup Policy to confirm requirements for daily backups and defined retention periods. Inspected backup logs and reports to verify backups are performed daily and retained in line with the predefined schedule. | No exceptions noted. |
| CC7.5 | All Day TA tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource. | Inspected tracking tool records and supporting evidence to verify that security deficiencies are logged, prioritized by severity, and independently reviewed. | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | | |
| CC7.5 | All Day TA ensures that incident response plan testing is performed on an annual basis. | Inspected documentation of the organization's incident response plan testing and reviewed evidence of the most recent annual test to confirm that the exercise was conducted in accordance with policy. | No exceptions noted. |
| CC7.5 | All Day TA has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company. | Inspected documentation identifying the incident response team and reviewed incident management records to confirm the team quantified and monitored incidents related to security, availability, processing integrity, and confidentiality. | No exceptions noted. |
| CC7.5 | All Day TA has implemented an Incident Response Policy that includes documenting Lessons Learned and "Root Cause Analysis" after incidents and sharing them with the broader engineering team. | Inspected the organization's incident response documentation to verify that lessons learned and root cause analysis were recorded following an incident exercise, and reviewed evidence that outcomes were communicated to relevant engineering teams. | No exceptions noted. |
| **Change Management** | | | |
| **CC8.1** The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives. | | | |
| CC8.1 | Separate environments are used for testing and production for All Day TA's application | Inspected system architecture documentation and environment configuration settings to confirm that separate environments are maintained for testing and production. | No exceptions noted. |
| CC8.1 | Only authorized All Day TA personnel can push or make changes to production code. | Inspected production environment access controls and code repository permissions to confirm that only authorized personnel have the ability to push or make changes to production code. Inspected access | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | records to verify that permissions are restricted to approved individuals. | |
| CC8.1 | When All Day TA's application code changes, code reviews and tests are performed by someone other than the person who made the code change. | Inspected code repository records and pull request histories to confirm that code changes are reviewed and tested by an individual other than the developer who made the change. | No exceptions noted. |
| CC8.1 | All Day TA has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes. | Enquired with the management regarding the control activity to ascertain that the control operates as described.<br><br>Inspected relevant artefacts to ascertain whether All Day TA has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes. | No exceptions noted. |
| CC8.1 | All Day TA uses a version control system to manage source code, documentation, release labeling, and other change management tasks. Access to the system must be approved by a system admin. | Inspected version control system settings and access records to verify that code and documentation changes are managed through the system and access is granted only with appropriate approval. | No exceptions noted. |
| **Risk Mitigation** | | | |
| **CC9.1** The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions. | | | |
| CC9.1 | All Day TA has an established Incident Response Policy that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing. | Inspected the organization's Incident Response Policy to verify its documented management responsibilities and procedures for responding to security incidents, and reviewed evidence of annual testing to confirm the plan was exercised. | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| CC9.1 | All Day TA has implemented an Incident Response Policy that includes creating, prioritizing, assigning, and tracking follow-ups to completion. | Inspected the organization's Incident Response Policy to verify it included procedures for creating, prioritizing, assigning, and tracking incidents through resolution, and reviewed a sample of incident tickets to confirm that follow-ups were tracked to completion. | No exceptions noted. |
| CC9.1 | All Day TA performs backups daily and retains them in accordance with a predefined schedule in the Backup Policy. | Inspected the Backup Policy to confirm requirements for daily backups and defined retention periods. Inspected backup logs and reports to verify backups are performed daily and retained in line with the predefined schedule. | No exceptions noted. |
| CC9.1 | All Day TA has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems. | Inspected the organization's Disaster Recovery Plan to verify that it was formally documented and approved by management, and reviewed the plan to confirm that it outlined defined roles, responsibilities, and detailed recovery procedures. | No exceptions noted. |
| CC9.1 | All Day TA utilizes multiple availability zones to replicate production data across different zones. | Inspected system architecture documentation and configuration settings to confirm that production data is replicated across multiple availability zones. Inspected evidence of recent replication status or logs to verify the process is operational. | No exceptions noted. |
| CC9.1 | All Day TA has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company. | Inspected documentation identifying the incident response team and reviewed incident management records to confirm the team quantified and monitored incidents related to security, availability, processing integrity, and confidentiality. | No exceptions noted. |
| CC9.1 | All Day TA has implemented an Incident Response Policy | Inspected the organization's incident response | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | that includes documenting Lessons Learned and "Root Cause Analysis" after incidents and sharing them with the broader engineering team. | documentation to verify that lessons learned and root cause analysis were recorded following an incident exercise, and reviewed evidence that outcomes were communicated to relevant engineering teams. | |
| **CC9.2** The entity assesses and manages risks associated with vendors and business partners. | | | |
| CC9.2 | All Day TA maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually. | Inspected the organization's vendor directory to verify that it included key vendors and their compliance reports, and reviewed evidence of annual reviews of critical vendor compliance reports performed by management. | No exceptions noted. |
| CC9.2 | All Day TA maintains a documented list of third parties and vendors that are authorized to receive or access PII. | Inspected the organization's documented list of third parties and vendors authorized to receive or access PII to verify it was maintained and current, and confirmed management oversight of the listing. | No exceptions noted. |
| **ADDITIONAL CRITERIA FOR AVAILABILITY** | | | |
| **A1.1** 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. | | | |
| A1.1 | All Day TA has implemented tools to monitor All Day TA's databases and notify appropriate personnel of any events or incidents based on predetermined criteria. Incidents are escalated per policy. | Enquired with the management regarding the control activity to ascertain that the control operates as described.<br><br>Inspected relevant artefacts to ascertain whether All Day TA has implemented tools to monitor All Day TA's databases and notify appropriate personnel of any events or incidents based on predetermined criteria. Incidents are escalated per policy. | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| A1.1 | All Day TA automatically provisions new server instances when predefined capacity thresholds are met. | Inspected system configuration settings and monitoring dashboards to confirm that new server instances are automatically provisioned when predefined capacity thresholds are reached. | No exceptions noted. |
| A1.1 | All Day TA authorizes designated member(s) with the autonomy to validate, change, and release critical security patches and bug fixes, outside of the standard change management process, when absolutely necessary to ensure security standards and availability of the systems. | Inspected the policy and procedures granting designated members authority to validate, change, and release critical security patches and bug fixes outside of the standard change management process. Inspected evidence of recent emergency patch activities to confirm such changes were appropriately authorized and implemented only when necessary to maintain security and availability. | No exceptions noted. |
| A1.1 | All Day TA uses a load balancer to automatically distribute incoming application traffic across multiple instances and availability zones. | Inspected system architecture documentation and load balancer configuration to confirm that incoming application traffic is automatically distributed across multiple instances and availability zones. Inspected monitoring dashboards to verify the load balancer is operational. | No exceptions noted. |
| A1.1 | All Day TA has implemented tools to monitor All Day TA's servers and notify appropriate personnel of any events or incidents based on predetermined criteria. Incidents are escalated per policy. | Inspected server monitoring tool configurations and sample alerts to confirm events and incidents are detected based on predetermined criteria. Inspected incident escalation records to verify that incidents are escalated according to policy. | No exceptions noted. |
| **A1.2** The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives. | | | |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| A1.2 | All Day TA has an automated email sent to appropriate personnel when the backup process fails. Failed backups are resolved in a timely manner. | Enquired with the management regarding the control activity to ascertain that the control operates as described.<br><br>Inspected relevant artefacts to ascertain whether All Day TA has an automated email sent to appropriate personnel when the backup process fails. Failed backups are resolved in a timely manner. | No exceptions noted. |
| A1.2 | All Day TA conducts annual BCP/DR tests and documents according to the BCDR Plan. | Inspected documentation of the organization's most recent BCP/DR test to verify it was performed in accordance with the Business Continuity and Disaster Recovery Plan and confirmed results were documented by management. | No exceptions noted. |
| A1.2 | All Day TA performs backups daily and retains them in accordance with a predefined schedule in the Backup Policy. | Inspected the Backup Policy to confirm requirements for daily backups and defined retention periods. Inspected backup logs and reports to verify backups are performed daily and retained in line with the predefined schedule. | No exceptions noted. |
| A1.2 | All Day TA has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems. | Inspected the organization's Disaster Recovery Plan to verify that it was formally documented and approved by management, and reviewed the plan to confirm that it outlined defined roles, responsibilities, and detailed recovery procedures. | No exceptions noted. |
| A1.2 | All Day TA utilizes multiple availability zones to replicate production data across different zones. | Inspected system architecture documentation and configuration settings to confirm that production data is replicated across multiple availability zones. Inspected evidence of recent replication status or logs to verify the process is operational. | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | | |
| **A1.3** The entity tests recovery plan procedures supporting system recovery to meet its objectives. | | | |
| A1.3 | All Day TA conducts annual BCP/DR tests and documents according to the BCDR Plan. | Inspected documentation of the organization's most recent BCP/DR test to verify it was performed in accordance with the Business Continuity and Disaster Recovery Plan and confirmed results were documented by management. | No exceptions noted. |
| A1.3 | All Day TA performs backups daily and retains them in accordance with a predefined schedule in the Backup Policy. | Inspected the Backup Policy to confirm requirements for daily backups and defined retention periods. Inspected backup logs and reports to verify backups are performed daily and retained in line with the predefined schedule. | No exceptions noted. |
| A1.3 | All Day TA authorizes designated member(s) with the autonomy to validate, change, and release critical security patches and bug fixes, outside of the standard change management process, when absolutely necessary to ensure security standards and availability of the systems. | Inspected the policy and procedures granting designated members authority to validate, change, and release critical security patches and bug fixes outside of the standard change management process. Inspected evidence of recent emergency patch activities to confirm such changes were appropriately authorized and implemented only when necessary to maintain security and availability. | No exceptions noted. |
| A1.3 | All Day TA has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems. | Inspected the organization's Disaster Recovery Plan to verify that it was formally documented and approved by management, and reviewed the plan to confirm that it outlined defined roles, responsibilities, and detailed recovery procedures. | No exceptions noted. |
| **ADDITIONAL CRITERIA FOR CONFIDENTIALITY** | | | |
| **C1.1** The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality. | | | |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | | |
| C1.1 | All Day TA ensures that all connections to its web application from its users are encrypted. | Inspected web application configuration settings and observed connections to confirm that all user traffic is encrypted in transit using HTTPS/TLS. | No exceptions noted. |
| C1.1 | Username and password (password standard implemented) or SSO required to authenticate into application, MFA optional for external users, and MFA required for employee users. | Inspected application authentication settings and documentation to verify that login requires standard credentials or SSO, and that MFA is configured in accordance with company requirements. | No exceptions noted. |
| C1.1 | All Day TA requires two factor authentication to access sensitive systems and applications in the form of user ID, password, OTP and/or certificate. | Inspected system configurations and authentication settings, and reviewed a sample of user access attempts to determine whether multi-factor authentication was required to access sensitive systems and applications. | No exceptions noted. |
| C1.1 | All Day TA establishes written policies related to retention periods for the confidential information it maintains. | Inspected the organization's Data Retention and Deletion Policy to verify that retention periods for confidential information were defined and reviewed evidence of management approval of the policy. | No exceptions noted. |
| C1.1 | Role-based security is in place for internal and external users, including super admin users. | Inspected system access configurations and role definitions to verify that role-based security is implemented for internal, external, and super admin users. Reviewed a sample of user accounts to confirm that access was provisioned in accordance with assigned roles. | No exceptions noted. |
| C1.1 | All Day TA has established a data classification policy in order to identify the types of confidential information | Inspected the organization's Data Classification Policy to verify it defined categories of confidential information and | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | possessed by the entity and types of protection that are required. | the required protection measures, and inquired with management to confirm the policy was communicated and implemented. | |
| C1.1 | All Day TA has a clean desk policy in place to ensure that documents containing sensitive data are not in public areas or laying on unattended employee work areas | Inspected the organization's Information Security Policy to verify that it included a clean desk requirement and inquired with management regarding enforcement practices to confirm that sensitive documents are not left unattended in public or employee work areas. | No exceptions noted. |
| C1.1 | All Day TA's new hire contracts include a non-disclosure agreement (NDA) | Inspected a sample of new hire employment contracts to confirm that they include a non-disclosure agreement (NDA). | No exceptions noted. |
| C1.1 | All Day TA's customer data is segregated from the data of other customers | Inspected the system's "Manage Organizations" interface displaying unique organization IDs and names to confirm that customer accounts are logically segregated within the platform, ensuring that each customer's data is separated from other customers' data. | No exceptions noted. |
| C1.1 | All Day TA maintains an accurate network diagram that is accessible to the engineering team and is reviewed by management on an annual basis. | Inspected the organization's network diagram to verify it accurately reflected the current environment, confirmed it was accessible to the engineering team, and reviewed evidence of annual management review. | No exceptions noted. |
| C1.1 | Storage buckets that contain customer data are versioned. | Inspected the configuration settings of storage buckets containing customer data to confirm that versioning is enabled. | No exceptions noted. |
| C1.1 | Appropriate levels of access to infrastructure and code review tools are granted to | Inspected a sample of user access records for new employees to confirm | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | new employees within one week of their start date. | appropriate access to infrastructure and code review tools was provisioned within one week of their start date. | |
| C1.1 | All Day TA has established formal guidelines for passwords to govern the management and use of authentication mechanisms. | Inspected the company's password policy and related documentation to confirm formal guidelines are established governing password complexity, expiration, and the use of authentication mechanisms. | No exceptions noted. |
| **C1.2** The entity disposes of confidential information to meet the entity's objectives related to confidentiality. | | | |
| C1.2 | All Day TA disposes of data securely upon expiration of the established retention periods or when no longer needed for legal, regulatory, and/or business reasons. | Enquired with the management regarding the control activity to ascertain that the control operates as described.<br><br>Inspected relevant artefacts to ascertain whether All Day TA disposes of data securely upon expiration of the established retention periods or when no longer needed for legal, regulatory, and/or business reasons. | No exceptions noted. |
| C1.2 | A termination checklist is used to ensure that system access, including physical access, for terminated employees has been removed within one specified time | Inspected the organization's termination checklist and related procedures to verify that a process exists to remove system and physical access upon employee termination. Noted that no terminations occurred during the period. | No exceptions noted. |
| C1.2 | All Day TA has formal policies and procedures in place to guide personnel in the disposal of paper documents containing sensitive data. | Inspected the organization's Data retention and deletion policy and procedures governing the disposal of paper documents containing sensitive data to verify that formal guidance was established and approved by management. | No exceptions noted. |

| Trust ID | Control Description | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| C1.2 | Storage buckets that contain customer data are versioned. | Inspected the configuration settings of storage buckets containing customer data to confirm that versioning is enabled. | No exceptions noted. |
| C1.2 | All Day TA has formal policies and procedures in place to guide personnel in the disposal of hardware containing sensitive data. | Inspected the organization's policies and procedures to verify that they included requirements for the secure disposal of hardware containing sensitive data. Noted that no hardware disposals occurred during the period. | No exceptions noted. |