Simulacra
Synthetic Data Studio

SYSTEM AND ORGANIZATION CONTROLS (SOC) 3 REPORT ON MANAGEMENT'S ASSERTION RELATED TO ITS

Simulacra Synthetic Data Studio Platform

Relevant to Security, Availability, and Confidentiality

For the period January 15, 2025 to April 15, 2025

TOGETHER WITH INDEPENDENT AUDITORS' REPORT

Prepared by:

Sensiba

Table of Contents

1. Independent Service Auditors' Report

To the Management of Simulacra Data, Inc. (Synthetic Data Studio)

Scope

We have examined Synthetic Data Studio's accompanying assertion titled "Assertion of Synthetic Data Studio Management" (assertion) that the controls within Synthetic Data Studio Platform (system) were effective throughout the period January 15, 2025 to April the15, 2025, to provide reasonable assurance that Synthetic Data Studio's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)* in AICPA*, Trust Services Criteria.*

Service Organization's Responsibilities

Synthetic Data Studio 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 Synthetic Data Studio's service commitments and system requirements were achieved. Synthetic Data Studio has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Synthetic Data Studio is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditors' Responsibilities

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

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.

- Assessing the risks that controls were not effective to achieve Synthetic Data Studio's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Synthetic Data Studio's service commitments and system requirements based on the applicable trust services criteria.

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

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

Inherent Limitations

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

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the 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.

Opinion

In our opinion, management's assertion that the controls within the Synthetic Data Studio Platform were effective throughout the period January 15, 2025 to April 15, 2025, to provide reasonable assurance that Synthetic Data Studio's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

San Jose, California

June 18, 2025

2. Assertion of Synthetic Data Studio Management

We are responsible for designing, implementing, operating, and maintaining effective controls within the Simulacra Data, Inc. (Synthetic Data Studio) Platform (system) throughout the period January 15, 2025 to April 15, 2025, to provide reasonable assurance that Synthetic Data Studio's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented in the section of this report titled, "Description of the Synthetic Data Studio Platform," (description) and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 15, 2025 to April 15, 2025, to provide reasonable assurance that Synthetic Data Studio's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus - 2022)* in AICPA*, Trust Services Criteria.*

Synthetic Data Studio's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in the accompanying system description.

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

We assert that the controls within the system were effective throughout the period January 15, 2025 to April 15, 2025, to provide reasonable assurance that Synthetic Data Studio's service commitments and system requirements were achieved based on the applicable trust services criteria.

Signed by Synthetic Data Studio Management

June 18, 2025

3. Description of the Synthetic Data Studio Platform

Company Background

Simulacra Synthetic Data Studio (SDS) is an AI platform for predictive real-time synthetic data generation and causal scenario modeling. With Simulacra, you can generate realistic synthetic data that enhances prior consumer and market research studies. Simulacra SDS uniquely allows customers to integrate new knowledge and information into prior research for new, up-to-date predictions and “what-if” scenario models.

Industries currently served by Simulacra SDS include market and consumer research, consumer products and goods, and ad/marketing tech.

Services Provided

Simulacra’s proprietary technology offers a powerful way to simulate real-world scenarios without relying on large, expensive datasets. It helps to fill gaps, create predictive models, and enhance research accuracy. Its Zero Shot approach eliminates hallucinations that plague other generative models.

Simulacra allows customers to:

- Update prior studies with conditional generation to drive continuous product innovation.
- Rebalance cohorts and attributes for any existing dataset.
- Dramatically lower the cost and time needed to conduct extensive research.
- Amplify and uncover insights into low incidence, hard-to-survey, or unobserved cohorts.

Simulacra runs Hosted Single Tenant Sessions. If the page is refreshed or closed, the container is irrecoverably deleted. Customer data is never saved to the platform.

Principal Service Commitments and System Requirements

Simulacra SDS designs its processes and procedures related to its platform to meet its objectives for synthetic data generation services. Those objectives are based on the service commitments that Simulacra SDS makes to user entities, the laws and regulations that govern the provision of Simulacra’s services, and the financial, operational, and compliance requirements that Simulacra has established for the services. The synthetic data generation services of Simulacra SDS are subject to the security and privacy requirements of state and local privacy security laws and regulations in the jurisdictions in which Simulacra operates. Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the Simulacra platform that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.

- Use of encryption technologies to protect customer data both at rest and in transit.

Simulacra establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Simulacra'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 have been documented on how to carry out specific manual and automated processes required in the operation and development of the Simulacra platform.

Components of the System

Infrastructure

The service is hosted in Amazon Web Services, Inc.'s (AWS) data centers using AWS infrastructure as a service offering. The infrastructure of the Service includes the following key components.

- Simulacra SDS's AWS S3 buckets are provisioned with object lifecycle policies that delete information after the record retention timeframes.
- Simulacra SDS utilizes AWS multi-availability zones in order to ensure information processing facilities are implemented with redundancy sufficient to meet availability requirements.
- Simulacra SDS leverages AWS AMI to manage and restrict the allocation and use of privileged access rights.
- Simulacra SDS leverages the identity management capabilities of Google Apps for Business and Google Workspace to manage the full life cycle of identities.
- Simulacra SDS utilizes AWS network and security implementations including, VPC, security groups, firewall whitelists, and CloudWatch monitoring to manage the security of network services.
- Simulacra SDS networks are segregated at the environment level, such that the "development" environment and production application environment run on independent SSL certificates and internal docker networking, even while running on the same EKS cluster.

Simulacra SDS utilizes AWS CloudWatch to monitor all cloud services, including managing and monitoring for technical vulnerabilities. All incidents are logged in the incidence response documentation.

Software

Simulacra SDS has established the Software Development Lifecycle Policy that details:

- The rules for the secure development of software and systems and
- The security testing and acceptance process.
- The requirement to separate development, test, and production environments

The process to select, protect, and manage test information

In practice, this policy is deployed through GitHub merge rules.

Simulacra SDS source code, development tool, and software library access is provisioned and managed by GitHub.

Simulacra SDS utilizes Infrastructure as Code for all configuration management activities. All infrastructure deployments are logged in Git via GitHub.

Simulacra SDS does not install software on operational systems, all of the organization's technology is managed in the cloud.

People

Simulacra SDS is currently a team of three people, one of which, the Founder and CEO, performs all technology development and infrastructure related actions. The other co-founder is the Chief Marketing Officer, and the other employee is a part time MBA intern.

Given the current size of the organization, information security roles and responsibilities are held by Simulacra SDS's CEO / CTO.

The CEO is responsible for all of Simulacra’s operations including, but not limited to:

- The design, development, maintenance, dissemination, and enforcement of the items contained in this policy and other ISP policies.
- Ensuring that the information security management system conforms to the requirements of ISO/IEC 27001:2022.
- Reporting on the performance of the information security program to top management to identify areas for continuous improvement (5.2d, 5.3b).

Data

Simulacra runs on an isolated single tenant container. Simulacra does not save or retain customer data after each active session. All uploaded and generated data within the application is deleted upon session completion.

Simulacra maintains an inventory of all information in a secure Dropbox folder. Simulacra does not save or retain customer data after each active session. All uploaded and generated data within the application is deleted upon session completion.

Due to the small size of Simulacra SDS, all information is entirely restricted and can only be accessed by current team members. As the company grows, the policy for classifying information will evolve in accordance with the Data Classification Policy.

Simulacra SDS has established the Personal Data Management Policy that dictates how PII is handled in the case current retention practices change.

Simulacra SDS does not own or maintain any physical assets.

Processes, Policies and Procedures

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

Simulacra SDS is a remote first organization and does not have a physical location in scope for the ISMS Plan. All information is stored digitally, and service is hosted on AWS servers.

Physical Security

All data is hosted by Amazon Web Services (AWS). AWS data centers do not allow Simulacra SDS employees physical access. At present, Simulacra SDS does not maintain any office space and all work is conducted remotely.

Logical Access

- Simulacra SDS leverages AWS AMI to manage and restrict the allocation and use of privileged access rights.
- Simulacra SDS leverages the identity management capabilities of Google Apps for Business and Google Workspace to manage the full life cycle of identities.
- Simulacra SDS has developed the Information Security Policy and System Access Control Policy that define the rules to control logical access to information and other associated assets.
- Simulacra SDS has deployed an employee onboarding / offboarding process that permissions access to restricted resources on an as needed basis.
- Simulacra SDS review access rights on an annual basis for a minimal set of applicable permissions relevant to employee or contractor roles and responsibilities.
- Simulacra SDS has developed the Information Security Policy and Vendor Management Policy that define processes to manage information security risks associated with the use of supplier products / services. No current suppliers have access to the Simulacra SDS information.
- Simulacra SDS utilizes Dropbox as the record retention and document control repository. Infinite version retention and version recognition capabilities are enabled and user access is provisioned on an as needed basis to active employees of the organization.
- Simulacra SDS source code, development tool, and software library access is provisioned and managed by GitHub.

Computer Operations – Backups

On a daily basis, Simulacra SDS captures snapshots of all S3 buckets to backup information.

Computer Operations – Availability

Simulacra SDS utilizes AWS multi-availability zones in order to ensure information processing facilities are implemented with redundancy sufficient to meet availability requirements.

Simulacra SDS is a remote first organization and does not have a physical location in scope for the ISMS Plan. All information is stored digitally.

Change Control

Simulacra SDS has established the Software Development Lifecycle Policy that details:

- The rules for the secure development of software and systems and
- The security testing and acceptance process.
- The requirement to separate development, test, and production environments
- The process to select, protect, and manage test information

In practice, this policy is deployed through GitHub merge rules.

Simulacra SDS has also established the Change Management Policy that the requirement to subject changes to information processing facilities to the change management procedures. In practice, this policy is deployed through GitHub merge rules or through the AWS interface, detailed in a change management form.

Data Communications

Simulacra SDS uses de-encryption and firewall whitelists to limit access to company data.

Simulacra SDS utilizes AWS CloudTrail and S3 for short and long term retention of logs that record activities, exceptions, faults and other relevant events.

Simulacra SDS utilized AWS CloudWatch to monitor all cloud services for anomalous behavior and for potential information security incidents.

Simulacra SDS does not currently allow the use of privileged utility programs on company provisioned computers or devices. This policy may be revisited at such time that a privileged utility program is deemed necessary.

Simulacra SDS utilizes AWS network and security implementations including, VPC, security groups, firewall whitelists, and CloudWatch monitoring to manage the security of network services.

Simulacra SDS networks are segregated at the environment level, such that the "development" environment and production application environment run on independent SSL certificates and internal docker networking, even while running on the same EKS cluster.

Simulacra SDS has established the Encryption Policy that details the rules for or the effective use of cryptography, including cryptographic key management. In practice, all disks and network traffic is encrypted.

Control Environment

<u>Integrity and Ethical Values</u>

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

Simulacra's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Simulacra'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, as well as by example.

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

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- The CEO will verify compliance with this Code through various methods (e.g. periodic manager reviews, tool reports, internal and external audits, and employee feedback).
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- As Simulacra Synthetic Data Studio employees, we should avoid conflicts of interest and circumstances that reasonably present the appearance of a conflict of interest, especially if it would create an incentive for you or present the appearance of an incentive for you, (whether directly or indirectly).
- Background checks are performed for employees as a component of the hiring process.
- Any employee who violates this Code may be subject to disciplinary action, up to and including termination of employment in addition to any civil and criminal liability.

Once each year, as a condition of the employee's employment, they are required to acknowledge that they have received the Code of Conduct and understand its rules. New employees will sign an acknowledgment when they start with the company. Basically, their annual acknowledgment confirms that:

- The employee reviewed the Code of Conduct and they are required to comply with the Code of Conduct; the employee will comply with the compliance policies and procedures, as well as policies and procedures related to their job responsibilities;
- The employee will report any questions or concerns about suspected or actual violations of the Code to their supervisor, anyone in management or Simulacra Synthetic Data Studio's Compliance Officer,
- To the best of the employee's knowledge, they haven't acted contrary to the Code of Conduct
- The employee has reported any potential conflicts of interest to the Compliance Department.

Commitment to Competence

Simulacra's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into the requisite skills and knowledge.

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

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.
- Training is provided to maintain the skill level of personnel in certain positions.

Management's Philosophy and Operating Style

Simulacra's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward information processing, accounting functions, and personnel.

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

- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings are held to discuss major initiatives and issues that affect the business as a whole.

Organizational Structure and Assignment of Authority and Responsibility

Given the current size of the organization, information security roles and responsibilities are held by Simulacra SDS's CEO / CTO.

Simulacra SDS is currently comprised of three team members. High levels of coordination and collaboration is required and therefore segregation of duties is not feasible and have not been defined at this point.

Human Resource Policies and Practices

Simulacra SDS maintains a "Culture" document that outlines the style of working and culture Simulacra attempts to maintain.

Simulacra SDS requires all new employees or contractors to enter into formal employment agreements. These contracts:

- Specify the employee/contractors requirement as it relates to protecting the information security and outlines requirements for confidential information.
- Specify the employee/contractors requirement as it relates to the information security responsibility of the party post termination or change of employment.
- Include confidentiality agreement and separate non-disclosure agreements can be agreed upon on an as needed basis.
- Current employment contracts are maintained in Dropbox for all active and former employees / contractors.
- At onboarding, and on an annual basis, all Simulacra SDS employees are required to take the Drata Security Awareness Training that aligns to the policies and procedures of the organization.

Risk Assessment Process

A key element of Simulacra Synthetic Data Studio's information security program is a holistic and systematic approach to risk management. The policy defines the requirements and processes for Simulacra Synthetic Data Studio to identify information security risks. The process consists of four parts: identification of Simulacra Synthetic Data Studio's assets, as well as the threats and vulnerabilities that apply; assessment of the likelihood and consequence (risk) of the threats and vulnerabilities being realized, identification of treatment for each unacceptable risk, and evaluation of the residual risk after treatment.

- The risk assessment process includes the identification of threats and vulnerabilities having to do with company assets.
- The first step in the risk assessment is to identify all assets within the scope of the information security program; in other words, all assets which may affect the confidentiality, integrity, and/or availability of information in the organization. Assets may include documents in paper or electronic form, applications, databases, information technology equipment, infrastructure, and external/outsourced services and processes. For each asset, an owner must be identified.
- The next step is to identify all threats and vulnerabilities associated with each asset. Threats and vulnerabilities must be listed in a risk assessment table. Each asset may be associated with multiple threats, and each threat may be associated with multiple vulnerabilities.
- For each risk, an owner must be identified. The risk owner and the asset owner may be the same individual.
- Once risk owners are identified, they must assess:
    - Impact for each combination of threats and vulnerabilities for an individual asset if such a risk materializes.
    - Likelihood of occurrence of such a risk (i.e. the probability that a threat will exploit the vulnerability of the respective asset).
    - Criteria for determining impact and likelihood are defined in the tables below.
- The risk level is calculated by multiplying the impact score and the likelihood score.

Information and Communications Systems

Given the current size of the organization, information security roles and responsibilities are held by Simulacra SDS's CEO / CTO.

Simulacra SDS is currently comprised of three team members. High levels of coordination and collaboration is required and therefore segregation of duties are not feasible and have not been defined at this point. Information and communication systems are therefore simple forms of Slack, email, and video conferencing / in person communications.

As the organization grows, formalized information and communication systems and processes will be implemented.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Simulacra's management performs monitoring activities 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.

On-Going Monitoring

Simulacra's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in Simulacra's operations helps to identify significant variances from expectations regarding internal controls. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel.

Reporting Deficiencies

Drata is utilized to document and track the results of on-going monitoring procedures. Procedures are maintained for responding and notifying team member of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held to review reported deficiencies and corrective actions.

Changes to the System in the Last 3 Months

No significant changes have occurred to the services provided to user entities in the 3 months preceding the end of the review date.

Incidents in the Last 3 Months

No significant incidents have occurred to the services provided to user entities in the 3 months preceding the end of the review date.

Criteria Not Applicable to the System

All relevant trust services criteria were applicable to the Synthetic Data Studio Platform.

Subservice Organizations

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

The following subservice organization controls should be implemented by AWS to provide additional assurance that the trust services criteria described within this report are met.

Security Category	
Criteria	*Controls expected to be in place*
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.	AWS is responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where the entity's system resides.
CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	
CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	
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.	
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	
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.	

Security Category	
Criteria	*Controls expected to be in place*
CC6.4 - The entity restricts physical access to facilities and protected information assets (e.g., datacenter facilities, backup media storage and other sensitive locations) to authorized personnel to meet the entity's objectives.	AWS is responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers where the entity's system resides.

Availability Category	
Criteria	*Controls expected to be in place*
A1.2 - The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	AWS is responsible for managing environmental protections within the data centers that house network, virtualization management, and storage devices for its cloud hosting services where the entity's system resides.

Synthetic Data Studio management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, Synthetic Data Studio performs monitoring of the subservice organization controls, including the following procedures

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

Complementary User Entity Controls

Synthetic Data Studio's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the SOC 2 Criteria related to Synthetic Data Studio's services to be solely achieved by Synthetic Data Studio 's control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Synthetic Data Studio's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the SOC 2 Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

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