Sync.com Inc.

System and Organization Controls (SOC) 3

Report on the

Pro Document Collaboration Platform

Relevant to Security

For the Period
June 1, 2021 to December 31, 2021

Together with
Independent Service Auditors' Report

Independent Service Auditors' Report

To the Management of Sync.com Inc. (Sync)

Scope

We have examined Sync's accompanying assertion titled "Assertion of Sync Management" (assertion) that the controls within Sync's Pro Document Collaboration Platform (system) were effective throughout the period June 1, 2021 to December 31, 2021, to provide reasonable assurance that Sync's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (*trust services criteria*).

Service Organization's Responsibilities

Sync 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 Sync's service commitments and system requirements were achieved. Sync has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Sync 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 American Institute of Certified Public Accountants. 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 Sync'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 Sync'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.

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 Sync's Pro Document Collaboration Platform were effective throughout the period June 1, 2021 to December 31, 2021, to provide reasonable assurance that Sync'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
March 22, 2022

Assertion of Sync Management

We are responsible for designing, implementing, operating, and maintaining effective controls within the Sync.com Inc. (Sync) Pro Document Collaboration Platform (system) throughout the period June 1, 2021 to December 31, 2021, to provide reasonable assurance that Sync's service commitments and system requirements relevant to Security were achieved. Our description of the boundaries of the system is presented in the section of this report titled, "Description of Sync's Pro Document Collaboration 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 June 1, 2021 to December 31, 2021, to provide reasonable assurance that Sync's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Sync'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 June 1, 2021 to December 31, 2021, to provide reasonable assurance that Sync's service commitments and system requirements were achieved based on the applicable trust services criteria.

Signed by Sync Management

March 22, 2022

DESCRIPTION OF SYNC'S

PRO DOCUMENT COLLABORATION PLATFORM

Company Background

Since 2011, Sync.com Inc. (Sync) has been on a mission to provide a safe space for the world to collaborate. Sync helps users securely store share and access their documents and files from anywhere.

In 2013, Sync announced the launch of Sync Pro, a fully integrated cloud file storage and document collaboration platform with ground-breaking encryption and privacy controls built-in. In 2016 Sync announced the launch of additional products to serve expanded customer markets: Sync Pro Solo and Sync Pro Teams. These solutions offer a secure, collaborative workspace for industries such as IT, Healthcare, Education, Legal, Finance, Government, Engineering, Life Sciences, Media & Entertainment, Professional Services, Content Creators and Non-Profits: businesses and organizations entrusted with protecting important, confidential data.

As of 2021, Sync is trusted by over 1.8 million users in over 180 countries worldwide, recognized by industry leaders and tech experts for delivering improved productivity, security and privacy in the cloud.

Services Provided

Sync Pro Solo is a secure file storage and document collaboration platform that offers features such as file sync, sharing, backup, version history, deleted file recovery, document previews and email-based customer service. Basic, Plus and Professional plans provide distinct feature sets tailored to different individual user needs.

Sync Pro Teams is a secure file storage and document collaboration platform that offers features such as file sync, sharing, backup, version history, deleted file recovery, document previews, priority customer service via email and phone. Additionally, Sync Pro Teams offers features designed for better multi-user management including an administrator account, centralized billing and role-based access controls. Standard, Plus, Unlimited and Enterprise plans provide distinct feature sets tailored to the needs of businesses, organizations and teams of any size.

Users can access files and work securely across any supported computer or device.

Principal Service Commitments and System Requirements

Sync designs its processes and procedures related to its platform to meet its objectives for cloud technology services and systems. Those objectives are based on the service commitments that Sync makes to user entities, the laws and regulations that govern the provision of Sync services, and the financial, operational, and compliance requirements that Sync has established for the services. The cloud technology services and systems of Sync are subject to the security and privacy requirements of state, province and local privacy security laws and regulations in the jurisdictions in which Sync 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 Sync 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.

Sync establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Sync'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 Sync platform.

Components of the System

Infrastructure

To provide Sync's Pro Document Collaboration Platform, encrypted file data is stored and replicated on infrastructure owned and operated by Sync, co-located at Cologix and Cogent datacenters located in Canada:

- Cologix DC provides bulk-storage for encrypted file data
- Cogent DC provides replica storage for encrypted file data

Additional data is processed by and stored in hosted infrastructure including Amazon Web Services (AWS) VPC to create segregated development, test and production (live) environments, AWS EC2 to provide API endpoints for Sync's desktop, mobile and web apps, and AWS RDS to store encrypted file meta data.

Software

Sync's Pro Document Collaboration Platform is implemented using Linux, Nginx, PHP, Node JS micro-services, ZFS, Mongo and MySQL technologies using well-understood performance, scalability reliability and security methodologies. System performance, security and network intrusion monitoring is managed via Nagios, Prometheus, Suricata and Wazuh.

People

Sync personnel are categorized by the following functional areas:

- Corporate: Executives, Senior Management, Legal, Compliance, Auditing, Finance and HR
- Operations: Sales, Marketing, Customer Service and Billing
- Information Technology (IT): Software Developers, DevOps, Database Administrators, Systems Administrators, Information Security, Quality Assurance (QA) and Project Managers.

All of Sync's personnel are recruited and managed according to the policies and procedures outlined in the *Processes, Policies and Procedures* section below.

Data

Data, as defined by Sync, constitutes the following:

- Encrypted file and file meta data
- Shared linked file data
- Customer account data
- Logs

Sync's Pro Document Collaboration Platform stores and processes encrypted file and file meta data without inspection; data is encrypted client side before it is uploaded to Sync and is not accessible by Sync personnel due to client-side encryption. Access to customer account data and logs is restricted to authorized personnel. All other data access requires corporate authorization or explicit end-user permission.

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 teams are expected to adhere to the Sync policies and procedures that define how services should be delivered.

Physical Security

Sync.com Inc.'s company facilities are protected by security cameras, zone-based card access control, and security personnel with a designated reception area. Zone access is restricted based on assigned roles and responsibilities.

Logical Access

Sync utilizes role-based security architecture and requires personnel to be authenticated prior to the use of any system resources. Resources are protected via Client-side Certificates, Google OAuth, SSH Keys, OTP Multi-factor Authentication, VPN and SSL secured connections.

Computer Operations – Backups

Customer data is backed up and replicated by Sync's operations team on infrastructure owned by Sync located in Toronto, ON, Canada. In the event of an exception, operations personnel perform troubleshooting to identify the root cause and then failover to the replica data set immediately or as part of the next scheduled backup job.

Computer Operations – Availability

Sync personnel and automated systems monitor capacity utilization of physical, network and computing infrastructure to ensure that service delivery matches service level agreements. Infrastructure capacity monitoring includes, but is not limited to:

- Data center space, power and cooling
- Disk storage space for data
- Network bandwidth

Sync has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. Incident response policies and procedures are in place to identify, report, and act upon system security breaches and other incidents.

Change Control

Sync maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Quality Assurance Testing (QA) and User Acceptance Testing (UAT) results are documented and maintained. Development and testing are performed in a testing environment that is logically separated from production.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. Sync has implemented a

patch management process to ensure contracted, customer and infrastructure systems are patched in accordance with vendor recommended operating system patches.

Data Protection

Redundancy is built into Sync's Pro Document Collaboration Platform infrastructure, ensuring there is no single point of failure. This includes redundancy at the firewall, router, server and data storage level. If a primary system fails, redundant hardware is available to take its place.

Network security

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized.

Penetration testing is conducted to measure the security posture of a target system or environment. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications and occurs from both outside (external testing) and inside the network.

Vulnerability scanning is performed internally using industry standard scanning technologies, testing hardware and software in an efficient manner while minimizing the potential risks associated with active scanning.

Boundaries of the System

The scope of this report includes Sync's Pro Document Collaboration Platform services designed, implemented, operated and managed by Sync. The Subservice Organizations section below outlines the scope of boundaries not included in this report.

Applicable Trust Services Criteria and Related Controls

Common Criteria (to the Security Category)

Security refers to the protection of:

i. information during its collection or creation, use, processing, transmission, and storage and
ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Control Environment

The control environment at Sync is the foundation for other areas of internal control. It sets the tone of the organization and influences the control behavior of its personnel.

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 Sync's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Sync'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 Sync has implemented in this area include:

- Formally documented organizational policy statements and codes of conduct
- Policies and procedures require employees sign an acknowledgment form
- A confidentiality statement agreeing not to disclose proprietary or confidential information
- Background checks are performed for employees as a component of the hiring process.

Commitment to Competence

Sync's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Specific control activities that Sync has implemented in this area include:

- Management considers the competence levels for roles, and translates required skills and knowledge levels into written position requirements
- Training is provided to maintain the skill level of personnel

Management's Philosophy and Operating Style

Sync's management philosophy and operating style encompass a broad range of characteristics, which includes a measured approach to taking and monitoring business risks, information processing, accounting functions, and personnel. Specific control activities that Sync has implemented in this area include:

- Management is briefed on regulatory and industry changes affecting the services

- 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

Sync's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Sync's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. Specific control activities that Sync has implemented in this area include:

- Organizational charts are in place to communicate key areas of authority and responsibility
- Organizational charts are communicated to employees and updated as needed.

Human Resource Policies and Practices

Sync'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 its proven track record for hiring and retaining top quality personnel which ensures the service organization is operating at maximum efficiency. Sync's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities. Specific control activities that Sync has implemented in this area include:

- New employees are required to sign acknowledgement forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment
- Evaluations for each employee are performed on an annual basis
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist

Risk Assessment Process

Sync's risk assessment process identifies and manages risks that could potentially affect Sync's ability to provide reliable services to user entities. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. Risks identified in this process include the following:

- Operational risk – changes in the environment, staff, or management personnel
- Strategic risk - new technologies, changing business models, and shifts within the industry
- Compliance – legal and regulatory changes

Sync attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with other leadership committees and senior management.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Sync's cloud technology services and systems; as well as the nature of the components of the system result in risks that the criteria will not be met.

Sync addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. As part of the design and operation of the system, Sync's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Information and Communications Systems

Information and communication are an integral component of Sync's internal control system. At Sync, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, contractors and personnel.

Regularly scheduled calls are held to discuss operational efficiencies. Management meetings are held to develop Sync's business plans and discuss KPI reporting and outcomes. Additionally, Strategic Council meetings are held to review and discuss Sync's business plans, entity-wide new policies, procedures, controls, and other strategic initiatives within the organization.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Necessary corrective actions are taken as required to correct deviations from company policies and procedures.

On-Going Monitoring

Sync'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. The goal of this process is to ensure legal compliance and to maximize the performance of Sync's personnel.

Reporting Deficiencies

The results of on-going monitoring are documented and tracked. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately.

Changes to the System in the Last 12 Months

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

Incidents in the Last 12 Months

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

Criteria Not Applicable to the System

All Common criteria were applicable to the Sync Pro Document Collaboration Platform.

Subservice Organizations

Sync'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 the trust services criteria related to Sync's services to be solely achieved by Sync control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Sync.

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

Subservice Organization – AWS		
Category	Criteria	Control
Common Criteria / Security	CC6.4	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.

Subservice Organization – Cologix		
Category	Criteria	Control
Common Criteria / Security	CC6.4	A manned reception desk is in place to monitor and control access to the entrance of the facility either by 24/7 coverage (Cologix employee) or by security provided by the building landlord.
		Personnel are assigned to predefined badge access security zones based on job responsibilities.
		Policies and procedures are in place to guide personnel in physical security activities.
		User access to the badge access system is reviewed on the monthly access reports / administrator reports.
		The badge access system logs access attempts traceable to specific badge access cards. Security personnel review the access log on an ad-hoc basis.
		Badge access lists are reviewed monthly to help ensure data center access remains limited to authorized employee and customer personnel.
		A badge access system is utilized to secure exterior and interior access to the office facility.
		Administrative access to the badge access software is restricted to authorized individuals.
		Granting access to systems for new employees is done through NetSuite onboarding by the authorized hiring manager.
		Operations personnel complete an access revocation ticket and revoke production systems access privileges as a component of the termination process.
		Digital surveillance cameras are in place to monitor and record activity throughout the data center.
		Visitors are required to register in a visitor log prior to accessing the data center facilities. Logs are reviewed on a monthly basis to ensure that the logs were filled out completely, and logs are retained at least 90 days.
		Employee access to the data center requires approval by the employee's immediate entity supervisor.
		Visitors to the facility's Meet Me Room (MMR) are tracked and documented by the MMR's access logs found in the MMR access cases.
		UPS systems and batteries are inspected, and preventative maintenance is performed on at least an annual basis.

Subservice Organization – Cologix		
Category	Criteria	Control
		Various cooling strategies are used depending on the building. Cooling solutions other than raised floor air distribution are also in use.
		Management performs an assessment to identify potential threats of disruption to systems including an assessment of the physical and environmental risks to the facilities.

Sync management, along with the subservice organizations, 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, Sync performs monitoring of the subservice organizations controls, including the following procedures:

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

Complementary User Entity Controls

Sync'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 trust services criteria related to Sync's services to be solely achieved by Sync control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Sync's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the trust services 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 Sync.
2. User entities are responsible for notifying Sync 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 Sync 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 Sync services.

6. User entities are responsible for providing Sync with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Sync of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.