xerox™

REPORT ON XEROX CORPORATION'S XEROX APP GALLERY SYSTEM RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY FOR THE PERIOD JULY 1, 2020 TO JUNE 30, 2021

SOC 3® - SOC for Service Organizations: Trust Services Criteria for General Use Report

COALFIRE CONTROLS

TABLE OF CONTENTS

SECTION 1

Independent Service Auditor's Report.....3

SECTION 2

Assertion of Xerox Corporation Management 6

ATTACHMENT A

Xerox Corporation’s Description of the Boundaries of Its Xerox App Gallery System.....8

ATTACHMENT B

Principal Service Commitments and System Requirements.....13

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Xerox Corporation ("Xerox")

Scope

We have examined Xerox's accompanying assertion titled "Assertion of Xerox Corporation Management" (assertion) that the controls within the Xerox App Gallery System (system) were effective throughout the period July 1, 2020 to June 30, 2021, to provide reasonable assurance that Xerox'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* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

Xerox 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 Xerox's service commitments and system requirements were achieved. Xerox has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Xerox 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 Auditor's 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 Xerox'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 Xerox'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 the Xerox App Gallery System were effective throughout the period July 1, 2020 to June 30, 2021, to provide reasonable assurance that Xerox's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Coalfire Controls LLC

Westminster, Colorado
August 20, 2021

SECTION 2

ASSERTION OF XEROX CORPORATION MANAGEMENT

Xerox Corporation
11000 Weston Parkway
Cary, NC 27513

Assertion of Xerox Corporation ("Xerox") Management

We are responsible for designing, implementing, operating and maintaining effective controls within the Xerox App Gallery System (system) throughout the period July 1, 2020 to June 30, 2021, to provide reasonable assurance that Xerox'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 attachment A 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 July 1, 2020 to June 30, 2021, to provide reasonable assurance that Xerox'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* (AICPA, *Trust Services Criteria*). Xerox'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 attachment B.

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 July 1, 2020 to June 30, 2021, to provide reasonable assurance that Xerox's service commitments and system requirements were achieved based on the applicable trust services criteria.

Gopi Tatachar
SR Director, Data Center Services
XDX Global Infrastructure & Production Support
Xerox Corporation

ATTACHMENT A

XEROX CORPORATION'S DESCRIPTION OF THE BOUNDARIES OF ITS XEROX APP GALLERY SYSTEM

TYPE OF SERVICES PROVIDED

Xerox Corporation (“Xerox” or “the Company”) provides technology that innovates the way the world communicates, connects, and works. Through a broad portfolio of technology and services, the Company provides essential back-office support that helps clients’ businesses work better.

The Xerox App Gallery System is a gateway to a collection of downloadable and installable applications designed to transform the handling of documents and data by simplifying time-consuming, repetitive, or complex processes. With these applications, Xerox ConnectKey technology-enabled printers or multifunction printers (MFP) become well-connected, simple-to-use, smart workplace assistants.

THE COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES

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

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

Infrastructure

The Company utilizes a third party to provide the resources to host the Xerox App Gallery System. The Company leverages the experience and resources of the hosting provider to quickly and securely scale as necessary to meet current and future demand. However, the Company is responsible for designing and configuring the Xerox App Gallery System architecture within the hosting facility to ensure the availability, security, and resiliency requirements are met.

Software

Software consists of the programs and software that support the Xerox App Gallery System (operating systems [OSs], middleware, and utilities). The list of software and ancillary software used to build, support, secure, maintain, and monitor the Xerox App Gallery System includes applications to perform the following business functions:

- Application monitoring
- Backup and replication
- Infrastructure monitoring
- Antivirus
- Intrusion detection
- Help desk, ticketing system

People

The Company develops, manages, and secures the Xerox App Gallery System via separate departments. The responsibilities of these departments are defined in the following table:

People	
Group/Role Name	**Function**
Executive Management	Responsible for overseeing company-wide activities, establishing and accomplishing goals, and managing objectives.
Engineering	Responsible for the development, testing, deployment, and maintenance of new code for the Xerox App Gallery System.
Global Security Services	Responsible for oversight of cyber security.
Global Purchasing	Responsible for subcontract vendor management and governance, including security and risk management considerations.
Product Management	Responsible for overseeing the product life cycle, including adding new product functionality.
Engineering Services & Support	Responsible for managing access controls, security, and operations of the production environment.
Human Resources (HR)	Responsible for onboarding new personnel, defining the roles and positions of new hires, performing background checks, and facilitating the employee termination process.

Procedures

Procedures include the automated and manual procedures involved in the operation of the Xerox App Gallery System. Procedures are developed and documented by the respective teams for a variety of processes, including those relating to product management, engineering, technical operations, security, information technology (IT), and HR. These procedures are drafted in alignment with the overall information security policies and are updated and approved as necessary for changes in the business, but no less than annually.

The following table details the procedures as they relate to the operation of the Xerox App Gallery System:

Procedures	
Procedure	**Description**
Logical Access	How the Company restricts logical access, provides and removes that access, and prevents unauthorized access.
System Operations	How the Company manages the operation of the system and detects and mitigates processing deviations, including logical and physical security deviations.

Procedures	
Procedure	**Description**
Change Management	How the Company identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
Risk Management	How the Company identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

Data

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

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

The Company has deployed secure methods and protocols for transmission of confidential or sensitive information over public networks.

The following table details the types of data contained in the production application for the Xerox App Gallery System:

Data	
Production Application	**Description**
Usage Information	The Company keeps track of user activity in relation to the types of services customers and their users use, the configuration of their computers, and performance metrics related to their use of the services.
Logging Data	The Company logs information about customers and their users, including Internet Protocol (IP) address. Log files are immutable records of computer events about an OS, application, or user activity, which form an audit trail. These records may be used to assist in detecting security violations, performance problems, and flaws in applications.
User or Account Data	The Company collects data from its employees, customers, users (customers' employees), and other third parties such as suppliers, vendors, business partners, and contractors. This collection is permitted under the terms of service and privacy policy (as well as other separate agreements with vendors, partners, suppliers, and other relevant third parties). Access to user or account data is controlled through processes for provisioning system permissions, as well as ongoing monitoring activities, to ensure sensitive data is restricted to employees based on job function.

SUBSERVICE ORGANIZATION

The Company uses a subservice organization for data center colocation and managed services. The Company's controls related to the Xerox App Gallery System cover only a portion of the overall internal control for each user entity of the Xerox App Gallery System. The description does not extend to the colocation services for IT infrastructure or managed services provided by the subservice organization.

Although the subservice organization has been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organization. Controls are expected to be in place at the subservice organization related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. The subservice organization's physical security controls should mitigate the risk of unauthorized access to the hosting facilities. The subservice organization's environmental protection controls should mitigate the risk of fires, power loss, climate, and temperature variabilities.

The Company management receives and reviews the subservice organization's SOC 2 report annually. In addition, through its operational activities, Company management monitors the services performed by the subservice organization to determine whether operations and controls expected to be implemented are functioning effectively. Management also communicates with the subservice organization to monitor compliance with the service agreement, stay informed of changes planned at the hosting facility, and relay any issues or concerns to the subservice organization.

ATTACHMENT B

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Commitments are declarations made by management to customers regarding the performance of the Xerox App Gallery System. Commitments are communicated in the Global Operations Agreement and the Xerox Privacy Statement.

System requirements are specifications regarding how the Xerox App Gallery System should function to meet the Company's principal commitments to user entities. System requirements are specified in the Company's policies and procedures.

The Company's principal service commitments and system requirements related to the Xerox App Gallery System include the following:

Trust Services Category	Service Commitments	System Requirements
Security	• The Company utilizes reasonable and appropriate physical, technical, and administrative procedures to protect customer data from unauthorized access, use, or disclosure. • The Company provides infrastructure and procedures associated with application-level security, including secure communications, data encryption, penetration testing, and monitoring of security events.	• Logical access standards • Employee provisioning and deprovisioning standards • Access review standards • Encryption standards • Intrusion detection standards • Risk and vulnerability management standards • Configuration management standards • Incident handling standards • Change management standards • Patch management standards
Availability	• The Company will ensure the hours of operation are targeted to authorized clients on a 24x7x365 basis outside of any scheduled maintenance windows. • The Company will ensure the service availability target is 99.9%. • The Company maintains appropriate policies, technologies, and procedures for storing, restoring, and recovering data and systems in order to ensure business continuity.	• System monitoring standards • Backup and recovery standards • Data redundancy
Confidentiality	• The Company will use a variety of security technologies and procedures to protect confidential data from unauthorized access, use and disclosure.	• Data classification standards • Retention and destruction standards • Data handling standards • Internal confidentiality standards • Information sharing standards