Ver 3.0

RICOH

Integrated Cloud Environment

Security White Paper

Ver 3.0

Table of Contents

1. Preface

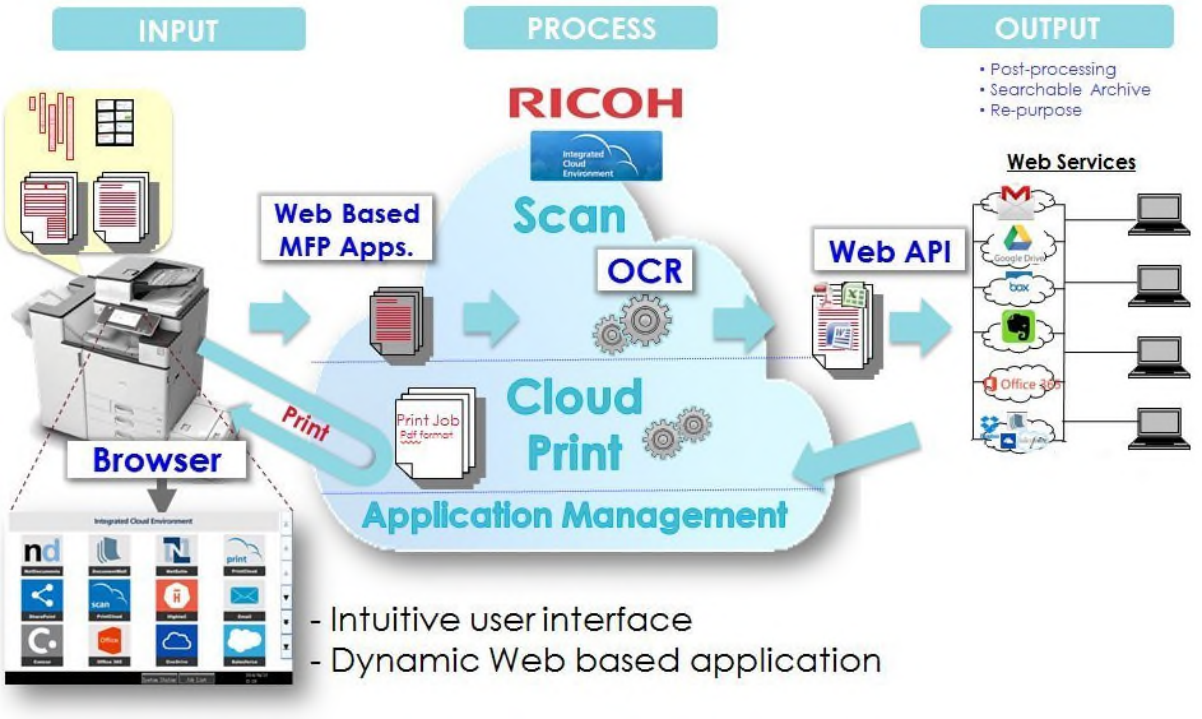
This guide provides the details of Security related information of Integrated Cloud Environment, describing important cloud hosting, data transfer and data backup information.

This page intentionally left blank to allow for duplex printing.

2. Introduction

What is Integrated Cloud Environment?

The Integrated Cloud Environment is a collection of Web applications running within the "Ricoh Cloud." An appropriate MFP device, with Browser Unit, is used to access these web applications. These web applications provide various document management services, like Scanning, OCR, Cloud Printing, and connectivity to popular document storage services.



3. System Overview

The Integrated Cloud Environment provides the necessary connectivity to access and utilize the available cloud services. This access is in conjunction with the OCR capability and Cloud Print capability also provided by the Integrated Cloud Environment.

The “core” or basic Integrated Cloud Environment components, including the web application server, OCR server, and the management platform server are hosted within a Microsoft Azure data center. The Print Cloud user application is an exception, and is powered by independently by Soonr Inc (www.soonr.com).

This Security White Paper will detail the security management incorporated in the basic Integrated Cloud Environment components.

Interacting with the applications

In order to ensure that any scanned document is stored or processed only by those authorized, Integrated Cloud Environment provides a “User Name and Password” authentication screen. This authentication is required whenever you scan your document to an external cloud service. Also once you hit the “Home” button, you are logged-out from the service, minimizing the risk of an application being used by anyone else. Additionally, if the “Home” button is **not** pressed, you are automatically logged-out from the session after 5 minutes.

Transmitting Information

All sensitive data transferred between the MFP and the Integrated Cloud Environment server, and between the Integrated Cloud Environment server and any external cloud service, is fully encrypted using 128 bit SSL. With the incorporation of encryption in all Integrated Cloud Environment communication, all users can be sure that the information and data being processed remains secure. Only image/icon files used for the user interface of the application are transmitted without encryption. This is done to improve the performance of the user interface rendering with the MFP Browser.

Understanding and Monitoring Usage

The Integrated Cloud Environment is able to monitor the user's scanning and printing activities at the Multi-Function Printer (MFP) to provide audit trail data. The activities which can be tracked are as follows:

Scanning from the MFP:

1. *Login Failure/Success*
2. *OCR Failure/Success*
3. *OCR File Upload Failure/Success*
4. *Scan File Upload Failure/Success*

Printing from the MFP:

1. *Download Failure*
2. *Invalid Release Code*
3. *Other Error*
4. *Print Success*

Ensuring Data is Secured

The Integrated Cloud Environment servers only store scanning and printing data for a temporary period in order to successfully transfer the data to its specified destination or to be downloaded to the MFP. The MFP local data is purged immediately after the transfer is complete.

All customer data used to manage their Integrated Cloud Environment license/accounts, such as: customer name, email address and admin name, is securely maintained and backed-up as detailed below.

Physical Security

The Integrated Cloud Environment is hosted at a secure Microsoft Azure data center located in Des Moines, Iowa (Azure designation: Central US). The data center provides unsurpassed security, and availability (up-time) for the application. The data center's security features include:

- Purpose-built data center with numerous prevention and detection technologies integrated into its architecture, including 24-hour security monitoring and control.
- Azure data centers are designed to the standards established by the National Fire Protection Association (NFPA). Specifically:
    - NFPA 75, Standard for the Protection of Information Technology (IT) Information Equipment, and
    - NFPA 76, Standard for the Fire Protection of Telecommunications Facilities

  These standards include specific requirements for data center construction, fire protection and detection systems, including gaseous, water mist and clean agent fire protection systems
- Proximity protection provided by 24-hour security guards, video surveillance, access controlled with biometric identification controls and mantrap corridors.

- Environmental Control cooling systems with monitored temperature humidity controls designed with n+1 reliability.

Data and Network Security

To protect against loss, corruption, or unauthorized access, the Integrated Cloud Environment's systems and procedures are designed and maintained for maximum security of all customer data. Among the security aspects of the Integrated Cloud Environment production systems and network are:

- Network perimeter defenses to prevent unauthorized access to the system and internal network, including firewalls and intrusion detection/prevention systems with 24-hour monitoring and event logging to identify and respond to potential threats.
- Multi-tiered system architecture to limit access and vulnerabilities due to security breaches.
- Compute Resource redundancy: all Azure virtual machines (VMs) are protected from failure by maintaining 3 redundant instances at all times. This prevents data loss
- Storage redundancy: data in Azure storage accounts are replicated to ensure durability and high availability. The ICE solution utilizes Locally-redundant storage (LRS). Every request made in the storage account is replicated three times. These three replicas each reside in separate fault domains and upgrade domains
- Hardened operating system on all production machines with regular security patching and vulnerability scanning.
- Virus protection to prevent malicious data corruption.

Systems Support

Integrated Cloud Environment system support is provided by a seasoned team of system and networking professionals certified in all key components of the physical production systems and Integrated Cloud Environment application. System personnel are available 24 hours a day, 7 days a week to ensure that the system remains accessible at all times. "Real-Time" systems monitoring is implemented to immediately notify the support staff should a problem occur.

Scheduled routine maintenance is performed to ensure the application is running optimally, and incorporates the latest software updates and upgrades including up-to-date protective measures, such as virus protection. All Integrated Cloud Environment systems are fully redundant to minimize the chance data of loss or corruption.

Operational and Process Security

To ensure maximum security in all phases of the Integrated Cloud Environment's development and support, Ricoh Americas Corporation incorporates a formalized set of "Information Security Management System (ISMS)" policies, and is ISO 27001 compliant. Developed by the International Organization for Standardization (ISO), ISO 27001 ensures that the guidelines and general principles for initiating, implementing, maintaining, and improving information security

management within an organization are maintained. To ensure compliance with defined procedures, regular audits are conducted.

Microsoft Azure

Microsoft Azure is a flexible, open, and secure public cloud built for business. Azure includes a broad collection of integrated services that accommodate many languages and operating systems. Services include:

- Compute
- Data Management
- Networking
- Developer Services
- Identity and Access
- Mobile
- Back-up
- Messaging and Integration
- Compute Assistance
- Performance
- Big Data and Big Compute
- Media
- Commerce

Microsoft Azure Data Centers

Microsoft Corp. delivers more than 200 cloud services including the Microsoft Azure platform. These services are hosted in Microsoft's cloud infrastructure composed of more than 100 globally distributed datacenters, edge computing nodes, and service operations centers. This infrastructure is supported by one of the world's largest multi-terabit global networks, with an extensive dark fiber footprint, that connects them all.

For more information visit www.microsoft.com/datacenters

Microsoft Azure Security and Compliance

Microsoft Azure has been developed to meet stringent security, privacy, transparency and compliance requirements. The Microsoft Azure infrastructure conforms to numerous certifications including ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2, ISO/IEC 27018. For a full list see https://www.microsoft.com/en-us/TrustCenter/Compliance/default.aspx"