PrintCloud

Security White Paper

Contents

1 Preface

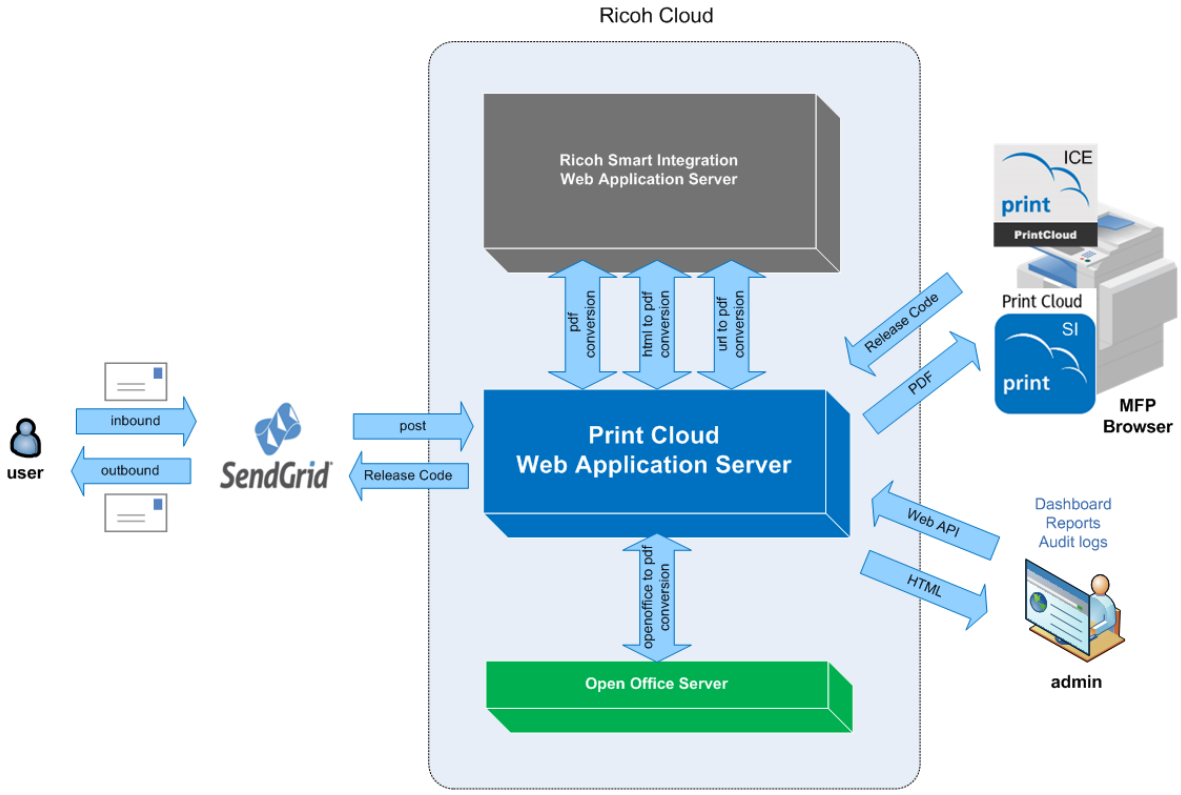
This guide provides the details of Security related information of PrintCloud, describing important cloud hosting, data transfer and data backup information.

2 Introduction

2.1 What is PrintCloud

The PrintCloud is a Web application which receives Print Jobs through Email. It converts Email body and attachments to PDF. It sends a release code to the sender of the email along with thumbnail. User gets separate release code for Email body and attachments. It also provides APIs to download the print job based on Release code, so that converted document can be printed on Ricoh MFP.

2 System Overview



The PrintCloud application is hosted within a Microsoft Azure data center. This Security White Paper will detail the security management incorporated in PrintCloud. Ricoh Smart Integration Web application Server is hosted in Amazon AWS. Refer to Ricoh Smart Integration Security White paper for Details.

Sendgrid, Cloud based email service is used for inbound email and outbound email delivery. Open Office Server is used to convert Open Office documents to PDF files.

2.1 Interacting with the application

User can submit print jobs by sending email to print@ricohprintcloud.com. Sendgrid parses the content and posts it to PrintCloud server though webhook. PrintCloud application further process the email, converts the email body and attachments to PDF by sending the contents to RICOH Smart Integration through encrypted TLS 1.2 protocol.

2.2 Transmitting Information

All sensitive data transferred between the MFP and PrintCloud server, and between the PrintCloud server and Smart Integration application Server, is fully encrypted using TLS 1.2 protocol. With the incorporation of encryption in all PrintCloud communication, all users can be sure that the information and data being processed remains secure. RICOH PrintCloud server uses a public key RSA 2048 bits and the certificate thumbprint algorithm SHA-256RSA

2.3 Email Transmission

When receiving a document as attachment by email, encrypted email is not supported. Also the emails sent from PrintCloud Server with release code are not encrypted. Customer need to make decision according to their security policy.

2.4 Understanding and Monitoring Usage

Converted Print Jobs are stored for a period of 7 days. After 7 days jobs are purged. Refer to next few sections for data security.

2.5 Ensuring Data is Secured

All customer data is securely maintained and backed-up as detailed below.

2.6 Physical Security

The PrintCloud is hosted at a secure Microsoft Azure data center. 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.

2.7 Data and Network Security

To protect against loss, corruption, or unauthorized access, the PrintCloud systems and procedures are designed and maintained for maximum security of all customer data. Among the security aspects of the PrintCloud 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.
- Hardened operating system on all production machines with regular security patching and vulnerability scanning.

Virus protection to prevent malicious data corruption.

2.8 Operational and Process Security

To ensure maximum security in all phases of the PrintCloud development and support, RICOH USA Inc. 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.

2.9 Penetration and Security test

Periodic Penetration and security tests are conducted using third party security assessment services as mandated by RICOH USA Inc. application security policies.

2.10 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

2.11 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

2.12 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"