RICOH TotalFlow™ Cloud

Security Overview

RICOH
imagine. change.

Table of Contents

1 Introduction 3

2 Keeping data safe and secured 4

Privacy 4
Customer Intellectual Property and Confidential Information 4
Confidentiality 4
Compliance 4
Secured Cloud Services 4

3 Securely controlling data access and transmission 5

Access controls 5
Interacting with RICOH TotalFlow Cloud 5
Authorized Personnel - Logging and Monitoring 6
Secured In-Transit Data Transfer 6
Data Storage and Encryption At Rest 6

4 Building safer applications and a solid infrastructure 7

Development Best Practices 7
Network Security 7
Vulnerability Scans and Patching 7

5 Protecting businesses with disaster recovery and business continuity 8

Information Security Plan 8
Third-Party Vendor Management 8

RICOH
imagine. change.

Introduction

Cloud Solutions for Production Environments: The next evolution of Ricoh software

Ricoh Company, Ltd., referred to as “Ricoh” in this document, is focused on connecting operational data, devices, processes and people to cloud-resident business intelligence tools. Moving data analytics to the cloud delivers significant advantages to Ricoh customers, including:

- Eliminating capital expense for server hardware
- Reducing costs associated with maintenance (updates to programs and operating systems)
- Access to on-demand expansion of system resources based on peak usage needs
- Use of a Software as a Service (SaaS) subscription model lowers upfront costs and assures access to the latest updates
- Built-in backup and disaster recovery capabilities

Leveraging a new model of secured, cloud-hosted technologies, the RICOH TotalFlow™ Producer and RICOH Supervisor™ products are designed to streamline the transformation of data into actionable business intelligence and information output that can be accessed quickly and easily.

A Security-First Approach

Ricoh understands the importance of keeping information secure, and that is why Ricoh solutions have security as a fundamental requirement during design, implementation and ongoing operations. This overview addresses Ricoh’s commitment to the important components of data and network security, providing customers the assurance they are looking for in their RICOH TotalFlow™ Cloud solutions.

Keeping data
safe and secured

Privacy

Ricoh prioritizes the protection of personal information. Details about the personal information Ricoh collects, uses, and retains is available in the Ricoh Privacy Policy.

Customer Intellectual Property and Confidential Information

Ricoh respects and protects the intellectual property (IP) of its customers and does not infringe upon the IP rights of customer information processed by RICOH TotalFlow Cloud. Ricoh is bound by its software contract to maintain the confidentiality of customer proprietary information.

Compliance

Ricoh monitors regulatory developments and updates practices to ensure the RICOH TotalFlow Cloud environment complies with regulatory obligations pursuant to applicable country, state and federal laws, as well as applicable industry rules and standards. When customers consider Ricoh as a partner, they should be confident that Ricoh applications meet their security, compliance and data processing needs.

RICOH TotalFlow Cloud has been SOC 2 Type 2 certified by Coalfire, an independent cybersecurity consulting firm. Click here to view the SOC 2 Certificate

Secured Cloud Services

The Ricoh cloud applications run on Amazon Web Services (AWS) which is an Infrastructure as a Service (IaaS) provider. For more information on AWS Compliance Programs, please refer to https://aws.amazon.com/compliance/programs/.

Securely controlling data access and transmission

Access Control

A user must login with a secure password to RICOH TotalFlow Cloud. Ricoh implements industry-standard password controls including:

Complexity

- At least 1 uppercase letter
- At least 1 lowercase letter
- At least 1 numeric digit
- At least 1 special character
- At least 8 characters

Expiration

- Password reset required for first login
- Password reset required every 60 days by default

Disallow reuse

- Last 12 passwords must be unique

Interacting with RICOH TotalFlow Cloud

All access to RICOH TotalFlow Cloud is via secure connections (e.g. HTTPS). A single administrator user login is created for each new customer account. The administrator user is responsible for creating additional customer logins with appropriate access for their roles. Role-based access applied throughout the system ensures each customer's administrators control what their users can (and cannot) see and do.

Ricoh protects customer data when providing consulting or maintenance services for RICOH TotalFlow Cloud by limiting access to authorized personnel on a need-to-know basis, by applying rules of least privilege when necessary, conducting quarterly reviews of permissions, and revoking access immediately following employee termination.

Authorized Personnel - Logging and Monitoring

User, system and network activity are logged to a protected centralized logging cluster. The centralized logs are ingested into a cloud-based Splunk solution where they are monitored by authorized personnel 24x7 and are analyzed and reviewed for anomalies and suspicious activity.

Secured In-Transit Data Transfer

All data in-transit, internal and to and from the cloud, are protected by strong cryptography and security protocols.

Data Storage and Encryption At Rest

Ricoh stores data in the cloud across multiple availability zones to ensure resiliency. Customer data is encrypted at rest using industry-standard encryption techniques.

Building safer applications and a solid infrastructure

Development Best Practices

The Ricoh development team employs secure coding techniques and development best practices, including, but not limited to:

- Code reviews
- Defect management
- Performance engineering
- Unit testing
- Agile programming
- Continuous integration

Developers are provided regular training in secure web application development practices. To avoid unwanted access within an application, Ricoh follows a least-privilege design approach to clearly define and separate duties (e.g. read-only versus read and write). For example, a service API can only query the one table it is allowed to query and has no access to other tables.

Non-production and production environments are separated. All code changes are peer reviewed and tested before they are deployed to production. The same change control process is followed for any changes to the environment itself.

Network Security

RICOH TotalFlow Cloud leverages AWS security features including AWS' Trend Micro Deep Security's Anti-Malware, Firewalls and Intrusion Prevention and AWS Security Groups to protect its network.

Firewall rules are configured to allow only what is needed for RICOH TotalFlow Cloud.

Externally exposed devices are part of Ricoh's controlled DMZ (demilitarized zone / perimeter zone), and Ricoh internet traffic is restricted based on IP geolocation. Ricoh's internal networks are logically and physically separated from AWS. Ricoh disables cloud services not required by Ricoh applications.

Vulnerability Scans and Patching

Ricoh employs a vulnerability management program focused on the remediation of security vulnerabilities and threats. Ricoh continuously monitors the cloud environment to maintain network security and identify potential risks, through random scanning, annual penetration tests, and by proactively applying needed patches.

Protecting business with disaster recovery and business continuity

Information Security Plan

Ricoh has adopted an information security plan that outlines Ricoh's security practices, policies and procedures, and which covers disaster recovery, service continuity and incident response.

A disaster recovery and service continuity plan provides for multiple availability zones and procedures to restore lost data from automated snapshots and is tested periodically. Backups are stored redundantly in multiple AWS secured data centers.

Ricoh's incident response plan is regularly tested and includes procedures related to initial response, investigation, communication, and remediation of security incidents.

Third-Party Vendor Management

To ensure compliance with applicable privacy and security requirements, Ricoh enters into appropriate confidentiality and data processing agreements with its vendors and business partners.

Should you have specific questions or concerns that are not addressed in this overview, please contact your Ricoh software representative. This document is an overview of the security approach and controls Ricoh applies to its products and services. Ricoh's specific security obligations to its customers are set out in the customer agreements entered into between Ricoh and its customers.

To learn how RICOH TotalFlow Producer and RICOH Supervisor, our vendor-neutral, secured cloud-based solutions can transform your business or to request a free trial, please visit www.ricohsoftware.com

RICOH
imagine. change.