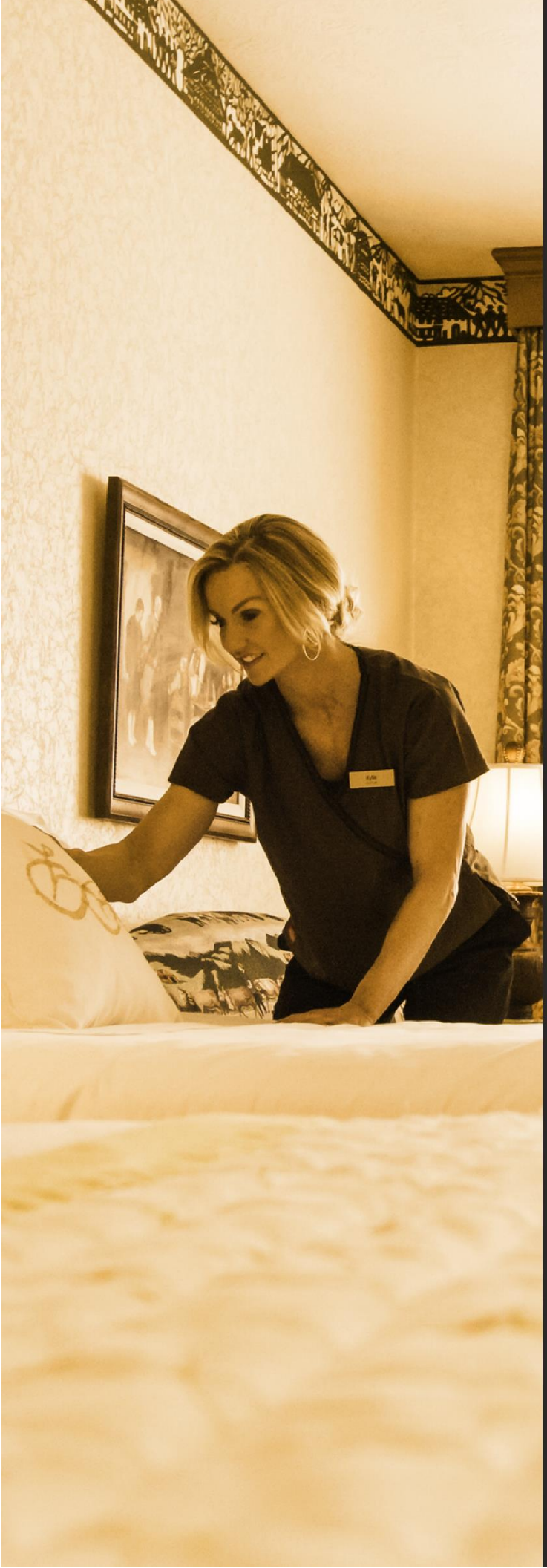


Security Practices and Policies

Management Console, Mobile Auditor And Enterprise Intelligence

Q1 2020

rizepoint

2890 East Cottonwood Parkway, Suite 250
Salt Lake City, UT 84121
(801) 285-9810

Contents

1 Introduction

It is the mission of the RizePoint Enterprise Security Office to provide an environment that protects and preserves the confidentiality, integrity, and availability of RizePoint customers' compliance management data. This document provides an overview of the policies and practices in place to inform and ensure customer confidence in the overall security of the RizePoint platform.

2 General Security Protections

2.1 Control and Compliance Environment

The RizePoint Enterprise Security Office (ESO) is chaired by the CTO (Chief Technology Officer) and consists of the Director of Information Technology and Principal Architect. Under the authority of the ESO, RizePoint maintains administrative, physical and technical safeguards to endeavor to protect its network and systems from security risks. RizePoint's data protection policies and procedures are then managed by the RizePoint IT team and Data team.

RizePoint IT monitors security for production systems. Policies and procedures are published and communicated to employees after ESO approval. These policies include, but are not limited, to the following:

- Access management
- Audit, logging, and monitoring
- Physical security
- Network and system security
- Risk assessment
- Disaster recovery
- Incident handling and response
- Software development and deployment

2.2 Security and Awareness Training

RizePoint maintains a security awareness program through annual security training. Standard security topics are communicated and all employees are required to complete online quizzes demonstrating knowledge. The following security principles are covered annually:

- Building (Physical) Security
- Phishing and Spear Phishing

- Access Policy (Bridget, Remote, VPN, etc)
- Clear Desk, Clear Screen
- Device Security
- Click Bait
- Passwords

In addition to these standard security topics, RizePoint performs internal security assessments that instruct the current and industry-relevant training. RizePoint designs this training around patterns identified in security monitoring, as well as annually-published industry research and breach reports.

3 Security Testing and Assessments

3.1 Application Penetration Test and Vulnerability Assessment

RizePoint conducts annual web application testing performed by third parties and performs web application testing itself on each new product version release. Additionally, RizePoint itself, or through a third party, conducts external penetration testing at least once annually. RizePoint provides customers with a copy of the summary results upon request. These tests are run against environments which exactly match production infrastructure, and include testing for all industry standards including OWASP Top 10.

3.2 SOC 2 Report

The RizePoint data center partner, ViaWest Delong, publishes a Service Organization Controls (SOC 2) Type II report. This report provides transparency into the data center safeguards in place, as defined by industry standards, which further demonstrates RizePoint's ability to protect customer data. This report is available by request.

3.3 PII (Personally Identifiable Information)

RizePoint does not house personally identifiable information such as credit cards or social security numbers. For this reason, RizePoint is exempt from compliance requirements as defined by PCI (Payment Card Industry Data Security Standard)

3.4 GDPR (General Data Protection Regulation)

Although RizePoint does not maintain an office in the European Union, customer data from those locations are processed by RizePoint infrastructure. For that reason,

RizePoint operates in accordance with the principles set forth by the EU for data consent, protection and right to be forgotten. RizePoint is currently in compliance with EU Safe Harbor and GDPR regulations. RizePoint operates an Enterprise Security Office and has an appointed Data Protection Officer to oversee compliance. More information about specific policies and controls can be reviewed by requesting a copy of "*RizePoint and GDPR – What you need to know*" (available under NDA only).

3.5 Risk Assessment

RizePoint conducts a formal risk assessment at least annually to review and evaluate its ability to appropriately address potential threats to its data and the data of its customers. These risk assessments include: Identification of Applicable Assets, Threat Identification, Risk Assignment and Scoring, and Risk Management. Risk analysis, in conjunction with industry trends and reports, contributes to the planning of security resources, control development, and other security safeguards at RizePoint.

4 Physical Security

4.1 Production Infrastructure

RizePoint's production infrastructure is currently hosted at an enterprise class data center. The hardware infrastructure is physically secured from other data center clients' hosted equipment. The hosting facility is secured and protected at a minimum N+1 redundant model for access/surveillance, power, fire suppression, HVAC, Internet connectivity/node room. The hosting facility is monitored and patrolled by NOC staff on a 24/7 basis. The hosting facility currently maintains SSAE 16 Type II certification.

4.2 Physical Access Controls

- In order to access corporate headquarters and the corporate server room, an electronic badge, with the correct access rights, is required.
- The corporate server room contains development servers as well as business-related servers and equipment. The server room is located at the corporate headquarters and is a dedicated room with access granted only to authorized personnel. The IT manager is responsible for granting or revoking access to the corporate server room.

- When an employee is terminated, physical access to all facilities is promptly revoked.
- Doors to all facilities require access badges for entry.
- In order for access to be granted or removed for new or terminated employees to corporate headquarters, IT must receive notification from the Human Resources (HR) department.
- Access to corporate headquarters and the corporate server room is logged. Logs are reviewed on an exception basis.
- The RizePoint corporate server room is protected from power outages using an Uninterruptible Power Supply (UPS) system.
- Only approved RizePoint technology employees are given physical access to the data center at corporate headquarters.

5 Data Center Hardening

5.1 Server Registration

A server/appliance is registered (i.e., serial # recorded in asset tracking system) and accepted by RizePoint IT before it is connected to an operational network. The RizePoint G&A team tracks these assets as best practice. Servers/appliances must have a proper DNS entry, both forward and reverse records. All RizePoint servers/appliances, whether production or non-production, are accessible only by authorized administrators. RizePoint installs and maintains current anti-virus software on applicable servers.

5.2 Server Hardening

RizePoint takes necessary steps to ensure the Operating System (OS) is kept secure, including but not limited to: changing default passwords, installation of security patches in a timely manner, and deactivation and/or de-installation of unnecessary software or services.

5.3 Storage Encryption

Physical drives within the Storage Area Network are encrypted using AES-256 in XTS cipher mode, which is a cipher mode designed specifically for storage. Both are FIPS 140-2 approved algorithms.

5.4 Business Continuity

RizePoint IT maintains a Business Continuity Plan commensurate with the impact of a failure or loss of the server, in accordance with RizePoint Disaster Recovery Policies. For more information about the RizePoint Disaster Recovery capabilities, please reference the document *"RizePoint Disaster Recovery"*, available at trust.rizepoint.com or by request from RizePoint customer support.

5.5 Monitoring

RizePoint enables monitoring checks for the appropriate software to ensure maximum uptime and quick response to problems. Network monitoring and graphing software establishes baselines for CPU, memory, network utilization and other computing resources. Monitoring software then aids in detecting anomalous use of resources which may indicate unauthorized behavior.

5.6 Network Security

RizePoint uses various tools to secure and continuously monitor network activity for the application and the internal systems and resources that support it. Events, including security incidents, are reported through these mechanisms for review and potential escalation. Secure and monitored endpoints and network connections provide the safeguards needed to protect the data of RizePoint and its customers from potential security threats.

6 Data Access

6.1 Password Policy and Controls

The RizePoint solution user account authentication and password information is stored in a one-way hash database. Password complexity can be configured by the Client and can be configured to require a minimum length of eight characters and consist of at least one uppercase alpha character, one or more lowercase alpha characters and one or more numeric characters.

6.2 Root Access

RizePoint keeps "root access" passwords in a secured and encrypted file available only to a small number of network operations personnel. These passwords are all at least eight characters and include varied special characters, numbers and letters and do not form words in any case. Authenticated SSH is required for direct server access by authorized RizePoint personnel. Remote access requires both a high

encryption VPN tunnel as well as authenticated SSH. The RizePoint solution user sessions currently time out after thirty (30) minutes of inactivity.

6.3 Data Partitioning

RizePoint utilizes a hybrid tenancy approach to data architecture. This means that customer specific data for the Management Console (the web application and customer reporting) is available for access by each client through a physically separated database. Reporting databases and BI tools utilize unique keys to partition customer data, preventing unauthorized cross-customer access.

6.4 Customer Access

RizePoint provides highly customizable access rules for various personas interacting with the RizePoint platform. Access controls can be defined by User, Organizational Group, Location or Role. The ability to control administrative functions such as adding new users, creating new inspection forms, or making permission changes are defined by these access policies.

RizePoint sets up individual SFTP folders for each customer that requires FTP access to import or export data. Each folder can be configured with its own security. If Secure FTP is not specified at login, access to the secured folder is denied.

6.5 Single Sign-On

RizePoint provides a centrally managed Single Sign-On (SSO) configuration that integrates RizePoint with existing corporate SSO solutions. Using this functionality, RizePoint easily plugs into the most popular SSO solutions, including Active Directory and other Federated solutions that support SAML 2.0. For more information on the RizePoint SSO solution, please refer to the *"RizePoint Technical Overview"*, available at trust.rizepoint.com and by request from RizePoint Customer Support.

6.6 RizePoint Employee Access

Access to RizePoint's internal and customer-facing network managed resources is governed by the Principle of Least Privilege—meaning that a user is only granted access to resources essential to his or her work responsibilities.

- Access by RizePoint Employees – The RizePoint Security Team determines each employee's responsibilities and subsequently restricts access to customer data and resources to the least amount necessary for the services

to be completed. Access granularity is established via a network of user profiles, or groups, divided into three categories:

  - Profiles/groups with no direct server access
  - Profiles/groups with direct server access
  - Domain Administrators

- New and Departing Employee Access Granting Policy – Prospective RizePoint employees who have successfully passed a mandatory background check are granted the appropriate level of access to physical and network managed resources determined by the RizePoint Security Team. No window of access to managed resources is granted to former RizePoint employees.

6.7 Mobile Access

The RizePoint platform can be accessed via mobile applications available on all major mobile platforms, or via mobile web. These applications provide an offline mode to remotely store data when internet connectivity is unavailable. All data is stored in a local database accessible only by the RizePoint application. Device level data encryption is available for iOS users, if password protection is enabled. For Android and Windows devices, the data encryption is also handled through their respective operating systems. Data transferred during download and upload is encrypted via SSL.

6.8 Data Classification Policy

The RizePoint team utilizes a data classification scheme that is straightforward and easily understood.

Category 4: Highly sensitive corporate and customer data that if disclosed could put the organization at financial or legal risk.

Example: Employee social security numbers, customer credit card numbers

Category 3: Sensitive data that if disclosed could negatively RizePoint or its customers.

Example: Contracts, customer information, audit results, IT infrastructure, employee reviews

Category 2: Internal data that is not meant for public disclosure.

Example: Sales contest rules, organizational charts, internal processes

Category 1: Data that may be freely disclosed with the public.

Example: Contact information, price lists

7 Change Management

RizePoint has established policies and procedures to set the standards for managing production and development change requests. All changes migrated to production are handled in a controlled manner and include review, testing, documentation, and version control. All change management requests are authorized by the RizePoint Change Control Board (CCB). RizePoint employees involved with CCB are trained on these policies and procedures. Changes to the RizePoint application are recorded in the CCB System.

8 Malicious Actor Protection

8.1 DDOS Mitigation

In computing, a distributed denial-of-service attack (DDoS attack) is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DDoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend the services of a host connected to the Internet. RizePoint utilizes hardware that provides a full suite of countermeasures to remove DDoS attack traffic while enabling the flow of legitimate traffic.

8.2 SQL Injection, Script attacks, Phishing, etc.

Our firewalls provide threat prevention capabilities that allow us to protect our network from attack despite evasive, tunneled, or circumvention techniques. The threat prevention features on our firewalls include security profiles that drop suspicious packets and support antivirus, anti-spyware, vulnerability protection, URL filtering, file blocking and data filtering capabilities.

8.3 Security Updates

Security vulnerability patches are evaluated against our installed system modules, software and utilities for their appropriateness and priority. Emergency patches are applied against our staging environment for fast evaluation and then to production during normal maintenance periods. Non-emergency preventative security patches are subject to full QA testing and approval prior to application in production during

normal maintenance periods. All security patches/fixes are applied under formal change control processes.

9 Incident Management and Response

The RizePoint Enterprise Security Office orchestrates the efforts of several departments within RizePoint to provide a secure environment for customers and their data. Even with adherence to industry best practices, policies, and procedures, not all security incidents are preventable. Therefore incident response is an important practice for rapidly detecting events and minimizing the loss of confidentiality, integrity, and availability of proprietary data.

9.1 Incident Definition

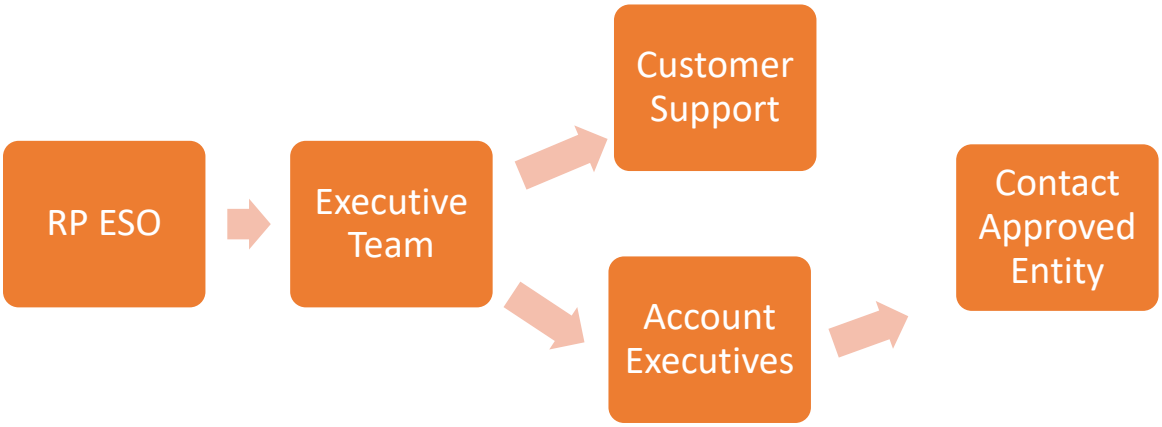
An incident is defined as any irregular or adverse event that occurs on any of the RizePoint networks, systems, or physical properties. These events typically either violate or will violate RizePoint security policies, acceptable use policies, or standard security practices. It is impossible to provide a comprehensive list of possible incidents. However, a few examples of possible incidents include: compromise of system integrity, denial of system resources, illegal access to a system, malicious use of system resources, or any type of damage to a system. RizePoint's policy addresses the following types and categories of incidents. Each area has specific guidelines on how Incident Responders are to analyze, contain, eradicate, and recover from an event such as:

- Unauthorized Access
- Denial of Service (DoS)
- Malicious Code
- Improper Usage
- Scans/Probes/Attempted Access
- Social Engineering
- Mobile Devices
- Theft/Loss of Assets
- Release or Disclosure of Information

9.2 Incident Notification Flow

When a security incident is declared, communication will flow from the RizePoint ESO to clients through the primary contact information on file. The information flow begins with the notification of a security incident by IT on staff. This information is circulated to the RizePoint executive team for review, and passed along through

Customer Support and the notification of individual account representatives. Affected customers will be notified within 24 hours of a declared security incident.



10 IP Addresses

RizePoint provides a unique URL for both a production and staging instance. Each of these URLs are backed by a non-unique IP. The URL for the production instance follows this naming convention: *yourcompanyname.RizePoint.com.* In this example, the URL for the staging instance would be: *yourcompanynametest.RizePoint.com.* Customers may determine the terminology for "yourcompanyname". All staging and production IP Addresses are secured and encrypted (SSL).

11 Disaster Recovery

RizePoint maintains a robust Business Continuity and Disaster Recovery plan. For more information, please refer to the document *"RizePoint Disaster Recovery"* at trust.rizepoint.com, or by request from RizePoint Customer Support.

12 Backups

RizePoint performs backups of data files from application systems. RizePoint maintains a formal Backup Policy, which applies to all critical systems, equipment, and data owned and operated by RizePoint. This includes all machines and hardware residing within its colocation facilities. This Policy includes sections addressing scope, policies,

procedures, and responsibilities as they relate to data backup and storage. RizePoint backups exist for database and file storage using a redundant backup strategy that includes local and off site backups in support of its contingency planning.

12.1 Backup Frequency

Full production and staging file (database and content storage) backups are created to disk on a weekly basis. Differential backups are performed on a daily basis. Log file backups are performed every 15 minutes. RizePoint nightly system backups are not customer-specific.

12.2 Access to Backup Data

Access to backups is managed and maintained through the controls established by RizePoint for controlling physical and logical access to sensitive data. Please see sections 4.2 and 6.5 regarding data access and physical security.

12.3 Restorations

The integrity of backup data is tested as part of the RizePoint Disaster Recovery Test plan. These tests are performed at least annually, using backups created during regular operation. These backups can also be used for purposes such as refreshing test databases, or restoring accidentally deleted files for customers. More information on data recovery procedures can be found in the document *"RizePoint Technical Overview"*, as well as the document *"RizePoint Disaster Recovery Plan"* available at trust.rizepoint.com or by request from RizePoint Customer Support.

13 Additional RizePoint Security Policies

13.1 Access Policy

RizePoint employees/contractors must first authenticate to the Company's corporate network (locally or through the VPN) using their Active Directory username and password before they can access relevant production systems and sensitive utilities. Once authenticated, employees can attempt to connect to system components in accordance with established access control levels as dictated by their personal profile. Upon doing so, they are then prompted to authenticate at the system layer using a username and password. Password parameters are configured on all relevant systems to include, where system functionality permits, settings such as minimum length, complexity, expiration, history, and lockout.

13.2 Password Policy

Password complexity requirements are enforced via Microsoft Group Policy. Character length is at least 8, uppercase, lowercase, and base 10 digits must all be used, last three passwords remembered cannot be used, rotated every 90 days. After 10 invalid login attempts the account is locked until unlocked explicitly by an administrator.

14 Conclusion

The contents of this document, as well as all Security Policy Procedures described herein and reviewed quarterly by the RizePoint Enterprise Security Office. With RizePoint, you get the simplicity of a world class software as a service solution, backed by the security your enterprise demands. Let RizePoint bring you peace of mind with comprehensive security features that help you protect your brand.

RizePoint.com