Rebalancing and trading due diligence

Keeping us all in control.

REDBLACK

Table of contents

This document addresses frequent questions and answers regarding our award-winning RedBlack Rebalancing and Trading product and services.

Every month, RedBlack Software receives numerous Request for Proposal (RFP) and Due Diligence (DD) questionnaires. For that reason, RedBlack provides a baseline of questions and answers to help you, our customers, understand our control environment around several topics such as security, operations, compliance, risk management and privacy.

The scope of this document applies to the RedBlack Rebalancing and Trading solution offered in the United States. If you have any questions regarding the information presented in this document or would like to receive information regarding other RedBlack products, please contact your account manager.

Privacy

01

Does RedBlack Software have a privacy program that ensures compliance with privacy laws and regulatory requirements related to maintaining security, confidentiality, processing integrity, and protection of customer information?

YES

02

Has a qualified individual been designated as a Data Protection Officer (DPO)?

YES

03

Are there privacy policies and procedures with identified privacy controls that are reviewed and revised at least annually?

YES

04

Is there a data privacy or data protection function that maintains enforcement and monitoring procedures to address compliance for its privacy obligations for customer privacy data?

YES

05

Is there a management procedure maintained to monitor changes in applicable privacy statutory, regulatory or contractual obligations?

YES

Audit and Risk

01

Are there policies and procedures to ensure compliance with applicable legislative, regulatory and contractual requirements?

YES

02

Is there an internal audit, risk management, or compliance department, or similar management oversight unit with responsibility for assessing, identifying and tracking resolution of outstanding regulatory issues?

YES

03

Does the audit function have independence from the lines of business?

YES

04

Is there non-audit staff dedicated to audit and risk responsibilities?

YES

05

Are there policies and procedures to address bribery, corruption, the prohibition of providing monetary offers or preventing improper actions that create advantage in practices with individuals and corporate representatives?

YES

06

Do employees receive training that covers anti-bribery and anti-corruption topics?

YES

07

Does RedBlack Software perform an annual SOC 2 Type 2 audit?

YES

Security policy

01

Is there a set of information security policies that have been approved by management, published and communicated to active employees and contractors?

YES

02

Are policies and standards based on industry accepted standards and practices?

YES

03

Is there a management-approved process for handling deviations and exceptions?

YES

04

Do the information security policies set requirements based on business strategy, regulations, legislation (including privacy and civil liberties obligations) and cybersecurity threat environment?

YES

05

Do the information security policies contain statements concerning the organization's definition of information security, objective, and principles to guide all activities relating to information security?

YES

06

Do owners review and update security policies if significant changes occur in legal, business, organizational, or technical conditions?

YES

Organizational security

01

Are responsibilities for asset protection and for conducting specific information security processes clearly identified and communicated to the relevant parties?

YES

02

Does the organization's executive leadership ensure information security policy is established and aligned with organizational strategy, and communicated to the entire organization?

YES

03

Has a qualified individual been designated as a Chief Information Security Officer (CISO) to oversee and implement the organization's cybersecurity program and enforce its cybersecurity policy?

YES

04

Does the CISO issue a report at least annually on the organization's cybersecurity program and material cybersecurity risks to the organization's board of directors, equivalent body, or senior officer in charge of cybersecurity risk?

YES

05

Are information security personnel (internal or outsourced) responsible for information security processes?

YES

06

Are information security personnel responsible for the design of information technology systems, processes, and architecture required to meet information security requirements?

YES

07

Do information security personnel maintain contacts with information security special interest groups, specialist security forums or professional associations?

YES

Application security

01

Is there an individual or group responsible for application security? YES

02

Are outside development resources utilized? YES

03

Is there formal software security training for developers? YES

04

Do all outside development resources comply with the SDLC (Software Development Life Cycle)? YES

05

Are development, test, and staging environment separate from the production environment? YES

06

Is there a formal Software Development Life Cycle (SDLC) process? YES

07

Does the SDLC process include integration testing, and acceptance? YES

08

Does the SDLC process include peer code review? YES

09

Is there a secure software development lifecycle policy that has been approved by management, communicated to appropriate active employees and contractors, and has an owner to maintain and review the policy? YES

10

Is there a documented change management/change control process for applications with customer data?

YES

11

Does the application change management/change control process include change control procedures required for all changes to the production environment?

YES

12

Does the application change management/change control process include management approval prior to deployment?

YES

13

Is a secure code review performed regularly?

YES

Network security

01

Is there a policy that defines network security requirements that is approved by management and has an owner to maintain and review?

YES

02

Is there an approval process prior to installing a network device?

YES

03

Is there a process that requires security approval to allow external networks to connect to the RedBlack Software network, and enforces the least privilege necessary?

YES

04

Are network intrusion detection capabilities employed?

YES

05

Are there security and hardening standards for network devices, including firewalls, switches, routers and wireless access points (baseline configuration, patching, passwords, access control)?

YES

Server security

01

Are server security configuration standards documented and based on external industry or vendor guidance?

YES

02

Are server security standards reviewed and/or updated at least annually to account for any changes in environment, available security features and/or leading practices?

YES

03

Are all systems and applications patched regularly?

YES

Cloud hosting

01

Are independent audit reports provided by the cloud hosting provider?

YES

Physical security

01

Is there a physical security program approved by management, communicated to active employees and contractors, and has an owner been assigned to maintain and review?

YES

02

Does the physical security program include a clean desk policy?

YES

03

Are there physical security controls for all secured facilities?

YES

04

Do the physical security controls include electronic controlled access system (key card, token, fob, biometric reader, etc.)?

YES

05

Do the physical security controls include digital CCTV with video stored at least 90 days?

YES

06

Are there physical access controls that include restricted access and logs kept of all access?

YES

07

Do physical access controls include collection of access equipment (badges, keys, change pin numbers, etc.) upon termination or status change?

YES

08

Are visitors required to sign in and out?

YES

End user device security

01

Are end user devices (desktops, laptops, tablets, smartphones) used for transmitting, processing or storing customer data?

YES

02

Are end user device security configuration standards documented?

YES

03

Are end user device security configuration standards reviewed and/or updated at least annually to account for any changes in environment, available security features and/or best practices?

YES

04

Are all available high-risk security patches applied and verified at least monthly on all end-user devices?

YES

05

Is there a mobile device management program in place that has been approved by management and communicated to appropriate employees and contractors?

YES

IT operations

01

Are management approved operating procedures utilized?

YES

02

Are operating procedures documented, maintained, and made available to all users?

YES

03

Is there an operational change management/change control policy or program that has been documented, approved by management, communicated to appropriate active employees and contractors and assigned an owner to maintain and review the policy?

YES

04

Do changes to the production environment including network, systems, application updates, and code changes subject to the change control process?

YES

05

Does the change control process include segregation of duties between those requesting, approving and implementing a change?

YES

06

Are integrity, availability and confidentiality specifications considered for new, upgraded or enhanced systems?

YES

Access control

01

Is there an access control program that has been approved by management, communicated to active employees and contractors, and has an owner to maintain and review the program?

YES

02

Are access control procedures reviewed periodically to keep up with changes in business environment, people, processes and technology?

YES

03

Is there a set of rules governing the way IDs are created and assigned?

YES

04

Are unique IDs required for authentication to applications, operating systems, databases and network devices?

YES

05

Is there a process to request and receive approval for access to systems transmitting, processing or storing RedBlack Software or customer data?

YES

06

Is there segregation of duties for granting access and approving access to RedBlack Software systems and customer data?

YES

07

Is access to systems that store or process customer data limited?

YES

08

Does the password policy define specific length and complexity requirements for passwords?

YES

09

Does the password policy require a minimum password length of at least eight characters?

YES

10

Are complex passwords (mix of upper case letters, lower case letters, numbers, and special characters) required on systems transmitting, processing, or storing customer data?

YES

11

Is multi-factor authentication deployed?

YES

12

Is multi-factor authentication required for privileged system access?

YES

13

Is multi-factor authentication available for customer accounts?

YES

14

Are employees and consultants access rights reviewed periodically?

YES

Asset and info management

01

Is there an asset management program approved by management, communicated to active employees and contractors and has an owner to maintain and review?

YES

02

Is there an asset Inventory list or configuration management database (CMDB)?

YES

03

Is there an acceptable use policy for information and associated assets that has been approved by management, communicated to appropriate active employees and contractorsand assigned an owner to maintain and periodically review the policy?

YES

04

Is there a process to verify return of constituent assets (computers, cell phones, access cards, tokens, smart cards, keys, etc.) upon termination?

YES

05

Is an owner assigned to all information assets?

YES

06

Is there a centralized key management system (KMS)?

YES

07

Is all customer data sent or received electronically encrypted in transit while on public and RedBlack Software SaaS networks?

YES

08

Does regulated or confidential customer data stored in a database include encryption at rest?

YES

Risk management

01

Is there a formalized risk governance plan that defines the Enterprise Risk Management program requirements?

YES

02

Does the risk governance plan include range of assets to include: people, processes, data and technology?

YES

03

Does the risk governance plan include range of threats to include: malicious, natural, accidental, cyber, business changes?

YES

04

Does the organization have a governing body accountable to maintain the risk governance plan?

YES

05

Is there a documented third-party risk management program in place for the selection, oversight and risk assessment of subcontractors (e.g., service providers, dependent service providers, sub-processors)?

YES

06

Does the third-party risk management program include assessments performed on all potential subcontractors before entering into contracts with them?

YES

Incident management

01

Is there an established incident management program that has been approved by management, communicated to appropriate active employees and contractors and has an owner to maintain and review the program?

YES

02

Is an incident / event response team available 24x7x365?

YES

03

Does the incident management program include an individual program owner?

YES

04

Is there a formal incident response plan?

YES

05

Does the incident response plan include guidance for escalation procedure?

YES

06

Does the incident response plan include a process for assessing and executing customer and third-party notification requirements (legal, regulatory and contractual)?

YES

07

Does the incident response plan require notifying the customer when unauthorized access to RedBlack Software systems and customer data is confirmed?

YES

Disaster recovery and business continuity

01

Is there an established disaster recovery and business continuity program that has been approved by management, communicated to appropriate active employees and contractors, and has an owner to maintain and review the program?

YES

02

Does the disaster recovery and business continuity program include an individual program owner?

YES

03

Is there a periodic (at least annual) review of your disaster recovery and business continuity procedures?

YES

04

Is there a formal, documented Information technology disaster recovery testing program in place?

YES

05

Are backups of RedBlack Software systems and customer data performed?

YES

06

Are backup and restoration procedures tested at least annually?

YES

Threat management

01

Is there an anti-malware policy or program that has been approved by management and has an owner to maintain and review the policy?

YES

02

Is there a vulnerability management policy or program that has been approved by management, communicated to appropriate constituent and an owner assigned to maintain and review the policy?

YES

03

Are network vulnerability scans performed against internet-facing networks and systems?

YES

04

Is penetration testing performed at least annually?

YES

05

Are penetration tests performed by independent trained and experienced personnel?

YES

Human resources

01

Are human resource policies approved by management, communicated to employees and an owner to maintain and review?

YES

02

Do Human Resource policies include background screening criteria?

YES

03

Are employees required to sign employment agreements?

YES

04

Do employment agreements include acknowledgement of acceptable use?

YES

05

Do employment agreements include acknowledgement of code of conduct / ethics policies?

YES

06

Do employment agreements include acknowledgement of confidentiality / nondisclosure policies?

YES

07

Does the security awareness training program include techniques to recognize phishing attempts?

YES

08

Does the security awareness training program include new hire and annual participation?

YES

09

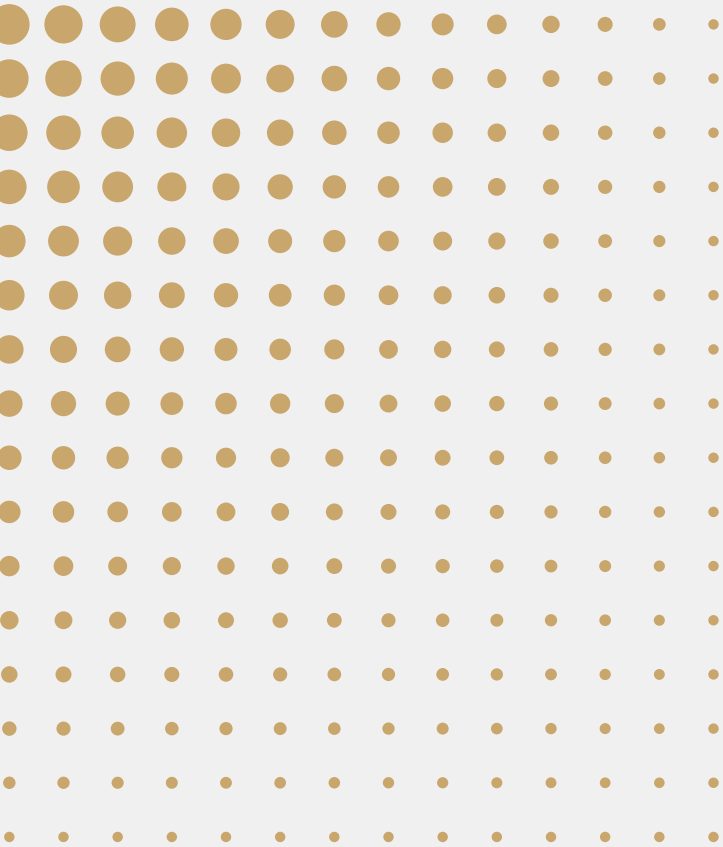
Does the human resource policy include termination and/or change of status processes?

YES

10

Is electronic access to systems containing customer data removed timely for terminated employees and contractors?

YES



REDBLACK

redblacksoftware.com

info@redblacksoftware.com