RISC CONSULTANTS

Cybersecurity Compliance

June 2022

CYBERSECURITY

In accordance with industry guidelines, RISC Consultants LLC (“RISC”, “us”, “we’) gives security and privacy the utmost importance. We do not sell or share your information with 3rd parties except with your consent, to comply with laws, to provide services pursuant to contracts, or to fulfill business obligations during everyday business

Responsibility	• President
Resources	• Internal and external systems, electronic devices, programs, etc. • Customer data
Frequency	• Annual: Identify risks • Annual: Conduct asset inventory • Ongoing: review integrity of systems, monitoring of breaches • Ongoing: Control of electronic devices/systems (passwords, retrieving/disabling devices held by terminated employees, etc.) • Annual: review of internal controls and procedures • Annual: provide report to senior management • Periodic: Train personnel on cybersecurity policies
Action	• Identify risks • Conduct asset inventory to identify critical assets and their vulnerability • Maintain a "whitelist" of trusted software to be used on Firm systems • Develop and update, as needed, a cybersecurity incident response program • Coordinate responses to intrusions and recovery • When necessary, confer with outside counsel, consultants, other experts • Develop and conduct employee training which may include meetings (electronic or otherwise) and policy reminders
Record	• Asset inventory • Control of Firm systems and devices • List of approved software to be used with Firm systems and devices • Records of intrusions and responses including reports to regulators, notification of customers, actions taken • Annual report to senior management • Records of training including date of training, persons trained, subjects included

This chapter outlines RISC’s program for addressing cybersecurity risks. These procedures are modeled after the NIST Framework for Improving Critical Infrastructure of Cybersecurity and are guidance for RISC. Procedures are subject to RISC’s business model and technology infrastructure.

Identification of Risks

Risks in RISC’s systems will be identified, reviewed annually, and updated when necessary, including the following:

- Identification of mission critical systems (email, data storage, etc.)

- Inventory of physical devices and systems, software applications and platforms (updated as necessary, particularly where new systems, software or devices are added)
- Prioritization of resources (hardware, data, and software) for protection based on their sensitivity and business value

Asset Inventory

The risk assessment will include an asset inventory to identify critical assets and their vulnerability to attack. RISC will also identify sensitive information and the location(s) where such information is stored. RISC will provide secured asset disposal, such as destroying hard drives of computers no longer in use.

Insider Threat

Responsibility	• President
Resources	• Insiders with access to critical systems and information
Frequency	• Annually
Action	• Identify insiders and update annually • Review potential malicious activity indicators
Record	• List of insiders

"Insiders" include individuals who currently have or previously had authorized access to RISC systems and data because of their function or role.

Insider's threats are addressed as follows:

- Identification of insiders and their access to firm systems and data

Identifying Potentially Malicious Activity

Malicious insider threats are challenging because these individuals know RISC and its systems and weaknesses. Indicators of potential risk, if known, may include notification or evidence of illegal activity; threats of retaliatory acts or violence; significant debt and recurring financial irresponsibility; time and attendance fraud; falsifying reports or records; unexcused or unauthorized absences; and other indicators of the employee's dissatisfaction that may lead to malicious activity.

To mitigate the potential for malicious activity, RISC has adopted the following practices:

- Cultivating a strong culture of compliance that encourages confidential reporting of potentially suspicious activity (e.g., "if you see something, say something")
- Designating a senior executive with responsibility for the firm's insider threat controls
- Providing timely notifications when access or privileges are changed or an employee resigns, or is terminated

Third Party Vendors

[Statement on Standards for Attesting Engagements (SSAE) No. 16; System and Organization Controls (SOC): https://www.aicpa.org/soc, https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/socforserviceorganizations.html]

Responsibility	• President
Resources	• Information about and provided by vendors • Vendor contracts • Services provided by vendors
Frequency	• Ongoing
Action	• Review the security controls of critical vendors through SOC2/SSAE report findings or through other appropriate methods (questionnaire, onsite review, annual meeting, etc.) • Follow up on any vulnerabilities identified for each vendor • Communicate vendor-issued security patches on a timely basis to users
Record	• Due diligence of vendor • Written contract • Reviews of vendor controls • Actions taken regarding vendor vulnerabilities

Third party vendors that will have access to RISC systems or devices will be reviewed, prior to engagement and periodically, to:

- Notify third party vendors to notify RISC of any breach of customer data
- Notify RISC Consultants of approved third party vendors and limitation of use to only approved vendors
- Periodically (at least annually) review security systems including cloud-based storage and protection of data

Data Loss Prevention (DLP)

A strong DLP program creates preventative controls that can help to detect and mitigate insider (and other) threats. DLP controls can prevent the inadvertent or malicious transmission of sensitive information to unauthorized recipients. DLP controls typically identify sensitive data based on rules and then block or quarantine the transmission of the data whether by email, data upload or download, file transfer or other method. RISC uses vendors to support these efforts including Zoho Corp & Google Drive.

RISC has adopted the following practices to prevent data loss:

- RISC subscribes to the enterprise versions of Zoho WorkDrive and Google Drive to ensure additional DLP features are available.

Retirement of Equipment Containing Data

Computers or other data-retaining equipment that will be disposed of will be subject to clearing of hard drives and other repositories of data prior to disposal. If a computer will be re-assigned to someone who is not authorized to view data stored on that computer, the hard drive will be cleared prior to reassignment. Flash drives and other portable data devices that will no longer be used or will be reassigned will be destroyed or cleared of all data prior to disposal or re-use.

Detection of Unauthorized Activity

Procedures to detect unauthorized activity on networks and devices include the following:

- Compliance settings are in place for any and all approved 3rd party software to monitor, detect and alert any perceived unauthorized activity.

Cybersecurity Incident Response Program

Responsibility	• President
Resources	• Evidence of intrusion, system anomalies
Frequency	• As required
Action	• Coordinate response and take actions included in this section • Notify clients as required
Record	• Records of intrusions and corrective action taken • Notices to clients as required

If an intrusion is identified, the designated cybersecurity supervisor will coordinate RISC's response which may include:

- Limiting access to affected systems or devices
- Diverting computer resources to a safe system
- Engaging a third party to process data until RISC's system is safe
- Engaging a third party to assess the intrusion
- Assessing data loss
- Notifying clients
- Evaluating potential financial losses
- Taking corrective action to prevent a future intrusion

Recovery

All RISC data is kept in secure cloud drives with additional compliance controls in place to ensure proper procedures for data backup and recovery of data.

Training

Data breaches may occur because well-intentioned employees or other users make preventable mistakes. Developing a firm culture that focuses on cybersecurity awareness and providing regular cybersecurity training can help address this problem. RISC provides ongoing training on:

- Sound practices regarding the opening of email attachments and links
- Identifying social engineering activities from hackers