RISC CONSULTANTS

Cybersecurity Compliance

CYBERSECURITY

RISC Consultants LLC ("RISC," "us," "we") prioritizes the security and privacy of client and employee information. We do not sell or share information with third parties except as required by law, with prior consent, or as necessary to provide contracted services or fulfill legitimate business obligations. This policy outlines RISC's approach to identifying, mitigating, and responding to cybersecurity risks.

Responsibility Overview

RISC's President is responsible for oversight of the cybersecurity program, with support from associates as needed. All personnel are responsible for adhering to the security practices outlined in this policy.

Identification of Risks

Annually, RISC will identify and review cybersecurity risks affecting our operations. This includes:

- Identification of mission-critical systems (e.g., email, data storage, accounting, and communication platforms)
- Inventory of physical devices, software applications, and platforms
- Prioritization of resources for protection based on sensitivity and business value

Asset Inventory

RISC maintains an asset inventory that includes all critical hardware, software, and cloud services. The inventory is updated whenever new tools are adopted or assets are retired. Retired devices are securely wiped or destroyed.

Insider Threat

An insider is any individual with authorized access to RISC systems and data. RISC mitigates insider threats by:

- Maintaining an up-to-date list of personnel with access to critical systems
- Reviewing access rights at least annually
- Encouraging confidential reporting of suspicious activity
- Promptly revoking access upon termination or role change

Third-Party Vendors

Vendors with access to client data or RISC systems are reviewed before engagement and periodically thereafter. Vendors must:

- Maintain security controls that meet industry standards
- Notify RISC within 24 hours of any data breach

- Limit use of RISC data to approved purposes only

Data Loss Prevention (DLP)

RISC uses secure, enterprise-grade cloud platforms with built-in DLP features to protect sensitive information. DLP rules and alerts are periodically reviewed to ensure ongoing protection.

Retirement of Equipment

All data-retaining devices are cleared or destroyed prior to disposal or reassignment, following NIST SP 800-88 guidelines. If destruction is performed by a third party, a Certificate of Destruction is obtained.

Detection of Unauthorized Activity

Approved software and systems are configured to detect and alert on unauthorized activity. Security logs are reviewed regularly, and suspicious activity is escalated for investigation.

Cybersecurity Incident Response

If an intrusion or security incident occurs, RISC will:

- Limit access to affected systems
- Engage external experts as needed
- Assess data loss and potential impact
- Notify clients and regulators as required
- Implement corrective actions to prevent recurrence

Recovery

RISC's data is stored in secure, backed-up cloud systems. Recovery procedures aim to restore operations within acceptable timeframes and minimize disruption.

Training

RISC provides cybersecurity training to all personnel at least annually, with additional reminders as needed. Training covers topics such as phishing awareness, password hygiene, and secure handling of client data.