https://www.aicpa.org/soc4so

CCR Information Security Assurance Attestation

www.ccr.net | 319.362.2384
845 Capital Drive SW Cedar Rapids, IA 52404

Security Assurance Statement

Commitment to Security and Compliance

Circle Computer Resources (CCR) is committed to protecting the confidentiality, integrity, and availability of information entrusted to us by our clients, partners, and employees. Security and compliance are foundational to CCR's operations and are integrated into governance, risk management, and day-to-day business processes.

CCR maintains a formal Information Security Program designed to support regulated, enterprise, and mission-critical environments and to align with applicable legal, regulatory, and contractual obligations.

Security Frameworks and Independent Assurance

CCR's Information Security Program is aligned with industry-recognized security frameworks and best practices, including:

- SOC 2 Trust Services Criteria (Security, Availability, Confidentiality)
- NIST Special Publication 800-53 security control principles
- CIS Critical Security Controls
- ISO/IEC 27001-aligned governance concepts

CCR has successfully completed an independent SOC 2 Type II examination, validating both the design and operating effectiveness of security controls over an extended review period. This examination provides independent assurance that CCR's security controls are operating consistently and as intended.

Information Protection Measures

CCR implements administrative, technical, and physical safeguards designed to protect sensitive and confidential information throughout its lifecycle. These measures are intended to:

- Protect the confidentiality, integrity, and availability of information
- Defend against reasonably anticipated threats and vulnerabilities
- Prevent unauthorized access, disclosure, alteration, or destruction of data

Security controls are applied consistently across CCR environments, while allowing flexibility to support business unit–specific operational requirements.

Security Governance and Oversight

CCR maintains formal security governance structures to ensure accountability, oversight, and alignment with business objectives. Governance practices include:

www.ccr.net | 319.362.2384
845 Capital Drive SW Cedar Rapids, IA 52404

- Defined security roles and responsibilities
- Executive oversight of information security activities
- Policy-driven control implementation and enforcement
- Periodic review of security objectives, risks, and performance

Information security policies are documented, approved by management, communicated to personnel, and reviewed periodically to ensure continued relevance and effectiveness.

Risk Management Approach

CCR employs a structured, risk-based approach to managing information security risks. This process includes:

- Identification of internal and external threats to systems and data
- Evaluation of risks related to technology, operations, regulatory requirements, and fraud
- Assessment of likelihood and potential business and data impact
- Prioritization of risks and definition of mitigation strategies

Formal risk assessments are conducted at least annually and updated as necessary based on changes to the business, technology environment, or threat landscape. Identified risks and mitigation activities are reviewed on a quarterly basis by the Security Team to support ongoing monitoring and informed decision-making.

This approach aligns with SOC 2 risk assessment and monitoring principles and reflects recognized risk management best practices.

Access Control and Identity Management

CCR enforces logical access controls designed to ensure that access to systems and data is limited to authorized individuals with a legitimate business need. Access control practices include:

- Role-based access and least-privilege principles
- Formal user provisioning and deprovisioning processes
- Periodic access reviews to validate appropriateness
- Authentication mechanisms appropriate to system sensitivity

Access rights are modified or revoked promptly upon role changes or termination to reduce the risk of unauthorized access.

System and Network Security

CCR maintains security controls to protect systems and networks from unauthorized access and malicious activity. These controls include:

- Network segmentation and firewall protections
- Secure system configuration standards
- Monitoring of security-relevant events
- Logging and alerting mechanisms to support detection and response

Systems are configured and managed to reduce exposure to known threats while supporting operational requirements.

Vulnerability and Patch Management

CCR maintains a vulnerability management program designed to identify, assess, and remediate security vulnerabilities in a timely manner. This program includes:

- Regular vulnerability scanning
- Evaluation of identified vulnerabilities based on risk
- Timely application of security patches and updates
- Tracking and remediation of identified issues

Vulnerability management activities are performed on an ongoing basis to reduce the risk of exploitation.

Security Awareness and Training

CCR promotes a security-conscious culture by ensuring personnel understand their security responsibilities. Security awareness measures include:

- Mandatory security awareness training for all employees
- Training covering topics such as phishing, data handling, and incident reporting
- Periodic reinforcement of security expectations

Training requirements are reviewed regularly to reflect evolving threats and organizational needs.

Incident Response and Security Events

CCR maintains documented incident response procedures designed to support timely detection, response, and recovery from security incidents. Incident response practices include:

- Defined roles and responsibilities
- Escalation and communication procedures
- Coordination with internal teams and third-party partners as needed
- Post-incident review and improvement activities

Security incidents are documented, investigated, and addressed in accordance with established procedures.

Physical and Environmental Security

CCR implements physical security controls to protect facilities and assets where systems or sensitive information are processed or stored. These controls include:

- Controlled access to facilities
- Environmental safeguards appropriate to the operating environment
- Physical protections aligned with the sensitivity of systems and data

Third-Party and Vendor Risk Management

CCR maintains a formal third-party risk management process to identify and manage risks associated with vendors, service providers, and business partners. This process includes:

- Maintaining an inventory of third-party relationships
- Categorizing vendors based on risk and access level
- Performing security due diligence during onboarding and periodically thereafter
- Incorporating security and confidentiality requirements into contracts

For higher-risk vendors, CCR may perform additional due diligence, including review of independent assurance reports such as SOC 2 Type II reports. Vendor risk is reassessed periodically and upon significant changes to the vendor relationship or service scope.

Continuous Monitoring and Improvement

CCR continuously evaluates the effectiveness of its security controls through:

- Ongoing monitoring activities
- Internal reviews and assessments
- Independent audit feedback
- Risk and incident analysis

Security controls and processes are updated as needed to address emerging threats, operational changes, and evolving business requirements.

Contact Information

For any questions or additional details regarding CCR's Information Security Program, please contact us directly legal@ccr.net.

www.ccr.net | 319.362.2384
845 Capital Drive SW Cedar Rapids, IA 52404