Coggno Inc.
SOC 2 Security Questionnaire Response

Executive Summary

Coggno Inc. maintains a security program designed to safeguard information assets and ensure the confidentiality, integrity, and availability of customer data. Security controls are aligned with the SOC 2 Trust Services Criteria and are continuously monitored and improved. The organization employs layered defenses including web application firewalls, network segmentation, access controls, encryption, logging, and regular patching. Cloud service providers are used in accordance with industry standards, and all system communications are encrypted. This document summarizes key security controls implemented by Coggno Inc.

Security (Common Criteria)

Control ID	Question	Response
CC6.1	Do you use a Web Application Firewall (WAF)?	Yes. Cloudflare WAF is implemented to mitigate DDoS attacks and OWASP Top 10 vulnerabilities.
CC6.2	How is infrastructure protected from internet exposure?	Internal servers are not publicly accessible. All traffic passes through load balancers, proxies, and security gateways.
CC6.3	How is access to servers controlled?	Server access is restricted using key-based authentication and limited to authorized personnel only.
CC6.6	Are firewall rules enforced?	Yes. Only required ports and services are exposed and all network traffic is monitored.
CC7.2	Do you monitor infrastructure?	Yes. Infrastructure endpoints, URLs, and logs are continuously monitored and reviewed.

Coggno

Availability

Control ID	Question	Response
A1.1	How do you ensure system availability?	Load balancers, modular services, and database mirroring provide redundancy and fault tolerance.
A1.2	Do you maintain backups?	Yes. Regular backups are performed and securely retained.
A1.3	Is disaster recovery implemented?	Yes. Disaster recovery procedures and system redundancy are in place.

Confidentiality

Control ID	Question	Response
C1.1	Is data encrypted?	Yes. Data is encrypted in transit using TLS/SSL and between internal services.
C1.2	How is access to sensitive data restricted?	Access is limited to authorized systems and personnel using role-based access control.

Processing Integrity

Control ID	Question	Response
PI1.1	How is system integrity ensured?	A modular application architecture with secure inter-service communication is enforced.
PI1.2	Are security headers implemented?	Yes. Industry-standard HTTP security headers are applied.

Privacy

Control ID	Question	Response
P1.1	How are user sessions secured?	Session timeouts are enforced and strong password policies are being implemented.

P1.2	Is role-based access implemented?	Yes. User access is provisioned based on defined roles and business need.
P1.3	How are user accounts managed?	User accounts are provisioned and deprovisioned based on authorization and operational requirements.

Third-Party Services

Control ID	Question	Response
TP1.1	Which cloud providers are used?	Cloudflare, Rackspace, Hetzner, and Amazon Web Services (AWS).
TP1.2	Are third-party communications encrypted?	Yes. All third-party communications are encrypted using industry-standard protocols.

Patch & Change Management

Control ID	Question	Response
CM1.1	How are systems patched?	Operating systems and applications are patched regularly following controlled procedures.
CM1.2	How are infrastructure changes controlled?	Infrastructure changes are reviewed and implemented under change management processes.

Logging & Monitoring

Control ID	Question	Response
LM1.1	Are logs collected?	Yes. System and access logs are centrally collected and retained.
LM1.2	Are alerts generated?	Yes. Alerts are generated for anomalous behavior and system failures.