SOC 2 Compliance Checklist

SOC 2 Compliance Checklist

SOC 2 is a voluntary compliance standard for service organizations, developed by the American Institute of CPAs (AICPA), which specifies how organizations should manage customer data. The standard is based on the following Trust Services Criteria: security, availability, processing integrity, confidentiality, and privacy.

This checklist is comprised of general SOC 2 requirements and does not constitute legal advice.

Compliancy Group

Need help completing your Checklist?

Speak with Compliancy Group

855-854-4722
info@compliancygroup.com

Establishing Security Policies & Procedures

□ Physical Access Controls
□ Logical Access Controls
□ System Monitoring
□ Incident Response Plans
□ Employee Training Programs

Conducting Regular Risk Assessments

□ Evaluating Threats
□ Analyzing Impacts of Threats
□ Implementing Appropriate Controls to Mitigate Risks

Implementing Access Controls

□ Multi-Factor Authentication
□ Role-Based Access Controls
□ Least Privilege Principles
□ Regular User Access Reviews

Ensuring Data Privacy

□ Collecting
□ Storing
□ Transmitting
□ Deleting

Monitoring & Logging

□ Track User Activities
□ Monitor System Performance
□ Detect Anomalies
□ Investigate Potential Security Breaches

Incident Response Planning

□ Identifying
□ Analyzing
□ Containing
□ Eradicating
□ Recovering

Vendor Management Controls

□ Conducting Due Diligence Assessments
□ Establishing Contractual Obligations for Data Protection
□ Regularly Monitoring Vendor Performance

Conducting Employee Training Programs

□ Data Protection
□ Privacy Regulations
□ Social Engineering Threats
□ Best Practices for Safeguarding Information