Venzip

SOC 2 COMPLIANCE *READINESS* GUIDE

For Startups & SaaS Companies

Venzip

1. SECURITY (Required — Common Criteria)

- [ ] **Access controls limit system entry to authorized users only**
  MFA, role-based access, SSO, principle of least privilege
- [ ] **Firewall and network security rules are configured and monitored**
  Intrusion detection/prevention systems active
- [ ] **Data encryption is applied at rest and in transit**
  TLS 1.2+, AES-256, encrypted backups
- [ ] **Security awareness training is conducted for all employees**
  At hire and annually; phishing simulations recommended
- [ ] **Incident response plan is documented and tested**
  Defined roles, escalation paths, communication protocols
- [ ] **Vulnerability management program is in place**
  Regular scanning, patching cadence, penetration testing
- [ ] **Change management process controls system modifications**
  Approval workflows, testing, rollback procedures
- [ ] **Risk assessment is performed and documented regularly**
  Identify threats, evaluate likelihood and impact, mitigate
- [ ] **Logging and monitoring captures security-relevant events**
  Centralized log management, alerting, retention policy
- [ ] **Vendor/third-party risk management process exists**
  Due diligence, contracts with security requirements

Venzip

2. AVAILABILITY

- [ ] **System uptime SLAs are defined and communicated to clients**
  Document target availability (e.g., 99.9%) and exclusions
- [ ] **Disaster recovery and business continuity plans are documented**
  RTO/RPO defined, tested at least annually
- [ ] **Backup procedures are automated and recovery is tested**
  Off-site/cloud backups with verified restoration
- [ ] **Infrastructure capacity is monitored and scaled proactively**
  Auto-scaling, performance baselines, alerting thresholds

3. PROCESSING INTEGRITY

- [ ] **Data processing is accurate, complete, and timely**
  Input validation, reconciliation checks, error handling
- [ ] **Quality assurance procedures validate system outputs**
  Automated testing, output monitoring, exception reporting
- [ ] **Error handling and correction procedures are documented**
  Defined process for identifying, logging, and resolving errors
- [ ] **Processing monitoring detects anomalies in real time**
  Dashboards, alerting rules, SLA tracking for processing jobs

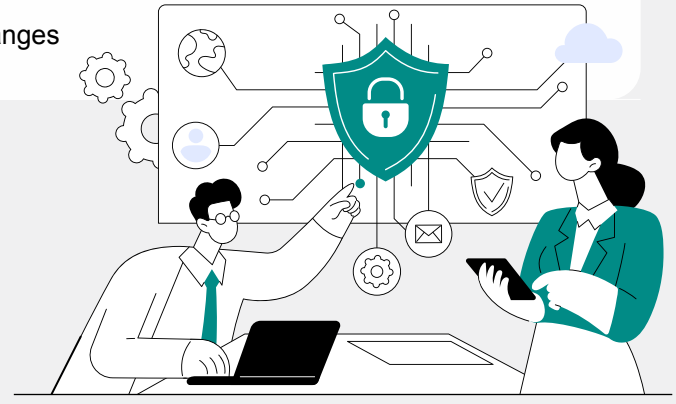
Venzip

4. CONFIDENTIALITY

- [ ] **Confidential data is classified and labeled**
  Data classification policy (public, internal, confidential, restricted)
- [ ] **Access to confidential information follows least privilege**
  Role-based access, regular access reviews, deprovisioning
- [ ] **NDAs and confidentiality agreements are in place**
  Employees, contractors, and third parties sign agreements
- [ ] **Data retention and disposal policies are enforced**
  Defined schedules, secure deletion, documented destruction
- [ ] **Encryption protects confidential data in storage and transit**
  Key management policy, rotation schedules, certificate tracking

5. PRIVACY

- [ ] **Privacy policy is published and accessible to users**
  Clear language on data collection, use, sharing, and retention
- [ ] **Consent mechanisms are in place for data collection**
  Opt-in/opt-out controls, cookie banners, preference centers
- [ ] **Personal data inventory maps all PII across systems**
  Know what data you collect, where it lives, and who accesses it
- [ ] **Data subject rights processes are documented and functional**
  Right to access, correct, delete, and port personal data
- [ ] **Privacy impact assessments are conducted for new features**
  Evaluate privacy risks before launching products or changes



READY TO GET SOC 2 COMPLIANT?

Venzip simplifies the entire SOC 2 journey — from readiness assessment to audit preparation.

Our AI-powered platform automates evidence collection, maps controls, and keeps you audit-ready.

REQUEST A DEMO


info@venzip.com


(604) 363-7138


www.venzip.com

Venzip