SOC 2 Information Security Policy Template

# 1. Purpose

This policy outlines the information security requirements and controls that our organization implements to meet the criteria of the SOC 2 Trust Services Criteria, specifically Security, Availability, Confidentiality, Processing Integrity, and Privacy.

# 2. Scope

This policy applies to all employees, contractors, and third parties who access our information systems and data. It covers all information assets, whether electronic, physical, or cloud-based.

# 3. Information Security Governance

* - Appoint a Chief Information Security Officer (CISO) or equivalent.
* - Establish an Information Security Management Committee.
* - Review and approve this policy annually.

# 4. Risk Management

* - Conduct annual risk assessments.
* - Document and track risk treatment plans.
* - Reassess risks after significant changes to systems or processes.

# 5. Access Control

* - Implement role-based access control (RBAC).
* - Require strong passwords and MFA for all systems.
* - Revoke access immediately upon employee termination.

# 6. Data Security and Confidentiality

* - Encrypt sensitive data at rest and in transit.
* - Restrict access to confidential data to authorized personnel only.
* - Maintain a data classification and handling policy.

# 7. System Operations and Monitoring

* - Enable system logging and monitor critical events.
* - Use intrusion detection/prevention systems (IDS/IPS).
* - Monitor uptime and availability metrics.

# 8. Change Management

* - Use a formal change control process for all production systems.
* - Document all changes with approval and rollback plans.
* - Test changes in a staging environment before deployment.

# 9. Incident Response

* - Maintain an Incident Response Plan.
* - Train staff on incident handling procedures.
* - Report incidents within defined timelines.

# 10. Business Continuity and Disaster Recovery

* - Maintain up-to-date BCP and DR plans.
* - Perform annual testing of recovery procedures.
* - Store backups securely and test their restoration.

# 11. Vendor and Third-Party Risk Management

* - Evaluate vendors’ security posture before engagement.
* - Sign data processing and security agreements.
* - Periodically reassess third-party compliance.

# 12. Training and Awareness

* - Provide annual security awareness training.
* - Track completion and effectiveness of training programs.
* - Include phishing simulations and other interactive content.

# 13. Policy Review and Updates

* - Review this policy annually or after major changes.
* - Communicate updates to all employees.
* - Maintain version control and documented approval.

# 14. Enforcement

* - Violations of this policy may result in disciplinary action.
* - Report suspected violations to the security team or HR.
* - Document and investigate policy breaches.