AUDIT VAULT

SOC-2 Policy Pack (Sample)

Confidential — For evaluation purposes only

Prepared by: Randal Quinn, Founder — Audit Vault
hello@auditvault.org | www.auditvault.org

What's inside this sample:

- Policy 1: Information Security Policy
- Policy 2: Access Control Policy
- Policy 3: Incident Response Plan
- *Policy 4+: Included in Foundation Audit*

Policy 1: Information Security Policy

Master Security Policy

Policy Owner	Approved By	Effective Date	Version
CTO	CEO	*[Date]*	1.0

1.0 PURPOSE AND SCOPE

This Information Security Policy establishes the framework for protecting *[Company Name]*'s information assets. It applies to all employees, contractors, interns, and third parties who access company systems or data.

- **Scope:** All information systems, networks, applications, and data owned or managed by [Company Name]
- **Who it applies to:** All personnel with access to company systems

2.0 SECURITY PRINCIPLES

Principle	Description
Least Privilege	Users receive only the access necessary for their role
Defense in Depth	Multiple layers of security controls are applied
Accountability	All access and actions are logged and attributable
Continuous Improvement	Security posture is reviewed and improved annually

3.0 ROLES AND RESPONSIBILITIES

Role	Responsibility
CEO / Founder	Ultimate accountability for the security program; approves this policy
CTO	Day-to-day security management; policy owner; provisions access
All Employees	Read, understand, and comply with all security policies; report incidents
Contractors	Comply with applicable policies; sign confidentiality agreements

4.0 COMPLIANCE AND ENFORCEMENT

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract. Suspected violations should be reported to the CTO.

5.0 REVIEW AND MAINTENANCE SCHEDULE

- This policy is reviewed **annually** by the CTO

- Major changes to systems or regulations trigger an out-of-cycle review
- All revisions are version-controlled and communicated to all employees

> *This is a sample policy. The full Information Security Policy — customized to your specific tools, infrastructure, and team — is included in the Foundation Audit.*

Policy 2: Access Control Policy

SOC-2 CC6 — Logical & Physical Access Controls

Policy Owner	Approved By	Effective Date	Version
CTO	CEO	*[Date]*	1.0

1.0 PURPOSE

This policy establishes requirements for managing user access to *[Company Name]*'s information systems. Access is granted on the principle of least privilege and reviewed regularly.

2.0 SCOPE

- All employees, contractors, and interns of *[Company Name]*
- All systems storing or transmitting company data, including *[AWS, GitHub, Google Workspace]*
- Third-party vendors with access to company systems

3.0 POLICY REQUIREMENTS

3.1 Access Request and Provisioning

1. User or manager submits request to CTO via *[email/Slack/ticketing system]*
2. CTO approves and provisions access within *[24/48]* hours
3. User acknowledges receipt of access in writing

3.2 Quarterly Access Reviews

Access is reviewed quarterly — by the 15th of January, April, July, and October. Unnecessary access is removed within 5 business days and documented.

3.3 Termination and Transfer (24-Hour Removal)

> **Critical:** All access must be removed within 24 hours of HR notification of departure.

1. HR notifies CTO of employee departure date
2. CTO disables all accounts within 24 hours
3. Access review confirms no lingering permissions

3.4 Multi-Factor Authentication (MFA)

- MFA required for **all** remote access to company systems
- Strong passwords meeting *[tool]* complexity requirements
- No sharing of individual accounts or credentials

3.5 Third-Party Access

- Must sign a confidentiality agreement before access is granted
- Access reviewed quarterly and removed within 24 hours when engagement ends

4.0 ROLES AND RESPONSIBILITIES

Role	Responsibility
CEO	Ultimate accountability for security program
CTO	Policy owner; approves/provisions access; conducts quarterly reviews
All Users	Comply with policy; report suspected unauthorized access
HR	Notify CTO of employee departures and transfers within same business day

5.0 DEFINITIONS

Term	Definition
Least Privilege	Granting only the access necessary to perform a job function
MFA	Authentication using two or more independent verification methods
Access Review	Periodic assessment of user permissions, documented and retained

Approved By (CEO)	Policy Owner (CTO)	Effective Date
_____	_____	_____
Signature / Name	*Signature / Name*	*Date*

Policy 3: Incident Response Plan

SOC-2 CC7 — System Operations

Policy Owner	Approved By	Effective Date	Version
CTO	CEO	*[Date]*	1.0

1.0 PURPOSE

This Incident Response Plan establishes the process for detecting, responding to, and recovering from security incidents affecting *[Company Name]*'s systems and data.

2.0 INCIDENT CLASSIFICATION

Level	Description	Response Time
🔴 **Critical**	Data breach, ransomware, complete system compromise	Immediate — 1 hour
🟠 **High**	Unauthorized access, significant data exposure	Same day — 4 hours
🟡 **Medium**	Suspicious activity, policy violation, minor exposure	Next business day
🟢 **Low**	Failed login attempts, minor anomalies	Within 5 business days

3.0 RESPONSE TEAM

Role	Name	Contact
Incident Commander	*[Name — CTO]*	*[Phone/Email]*
Security Lead	*[Name — Founder]*	*[Phone/Email]*
Communications Lead	*[Name]*	*[Phone/Email]*
External Counsel	*[Legal Firm Name]*	*[Phone/Email]*

4.0 RESPONSE PHASES

Phase	Actions
1 — Preparation	Maintain IR plan, conduct annual tests, train team
2 — Detection	Monitor alerts, identify and validate the incident
3 — Containment	Isolate affected systems; preserve evidence
4 — Eradication	Remove malicious code or unauthorized access; patch vulnerabilities

5 — Recovery	Restore systems; verify integrity before returning to production
6 — Post-Mortem	Document lessons learned; update controls within 30 days

5.0 COMMUNICATION PLAN

- Internal: Notify CTO immediately; CEO within 1 hour of Critical/High incidents
- Customers: Notify affected customers within **72 hours** per applicable regulations
- Regulators: As required by applicable law (e.g., GDPR, CCPA)

6.0 ANNUAL TESTING REQUIREMENT

This plan must be tested annually through a tabletop exercise or simulated incident. Results are documented and

> *This is a sample Incident Response Plan. The full version — customized to your specific infrastructure, tools, and team — is included in the Foundation Audit.*

used to update the plan.

Additional Policies

Included in Full Foundation Audit

Full Policy Pack (5–7 policies customized to your startup) is included in the Foundation Audit.

Each policy is written specifically for your team, tools, and infrastructure — not generic templates. Delivered in editable format so you can maintain them after the engagement.

Remaining policies in the full pack:

- *Change Management Policy*
- *Vendor Management Policy*
- *Business Continuity Plan*
- *Data Classification Policy*
- *Encryption and Key Management Policy*

Like what you see?

The full Policy Pack (5–7 policies, customized to your startup) is included in the Foundation Audit. Book a free strategy call to learn more.

Book a free 15-minute strategy call:

https://calendly.com/rqdevops76/15min

hello@auditvault.org | www.auditvault.org