

Company Vault & Policy Studio

For: compliance managers & primary contacts (Pro plan) · auditandcomply.com · July 2026

Who this guide is for: the people who own their company's policies. Vault mutations need a **manager role** (admin/compliance manager) or being the **lead contact**. Requires the Pro plan; a lapsed plan leaves everything readable, nothing editable.

1. The Company Vault: policies governed like evidence

Audit and Comply
VENDOR COMPLIANCE

[Dashboard](#)
[Assessments](#)
[Vendors](#)
[Compliance](#)
[Vault](#)
[Readiness](#)
[Standards](#)
[Network](#)
[Team](#)
[Billing](#)
[Notifications](#)

Sipho Dlamini
ADMIN

Sign out

Company Vault

Add a policy document

Title

Description

Document (PDF/PNG/JPG) No file chosen

DOCUMENT	STATUS	NEXT REVIEW	OBLIGATIONS
Acceptable Use Policy	DRAFT	—	0
Incident Response Plan	APPROVED	2027-06-25	1

The Vault: each card is one governed policy with its lifecycle state, next review date and recurring obligations.

A vault document is more than a file. It has a **lifecycle** (Draft → Awaiting approval → Approved → Retired), **version history**, a **review cycle** with reminders, and **obligations** — the recurring duties the policy commits you to. Where your team has two or more people, approval requires someone other than the submitter (four-eyes); solo teams record a self-approval.

2. Policy Studio: generate the policy you're missing

Audit and Comply
VENDOR COMPLIANCE

Dashboard
Assessments
Vendors
Compliance
Vault
Readiness
Standards
Network
Team
Billing
Notifications

Sipho Dlamini
ADMIN
Sign out

Generate a policy

Pick what your business is missing. The AI drafts it from your company profile; you edit and approve before it counts as evidence. AI-drafted — not legal advice.

Information Security Policy

The umbrella policy: management commitment, roles, and the security principles every other control hangs off. The document most assessments ask for first.

JS2 2024 s6.1.5 · POPIA s19 · ISO A.5.1

Generate

Incident Response Plan

Who does what when something goes wrong: detection, containment, communication (including regulator and customer notification), and post-incident review.

JS2 2024 s7.5 · POPIA s22 · GDPR Art 33

Generate

Access Control & Password Policy

Joiner/mover/leaver access, least privilege, MFA, password rules, and periodic access reviews.

JS2 2024 s8.1-8.3 · ISO A.5.15

The catalog: eight policy types that assessments actually ask for. Each knows its structure, its intake questions and the obligations it should install.

Don't have an incident response plan? Generate one. Two ingredients make the draft genuinely yours:

- 1 **Your company profile** — industry, headcount, systems (Microsoft 365? AWS?), data types, key contact. Fill it once under Portal → Company profile.
- 2 **Two-to-four intake questions** specific to the policy — for an IR plan: who leads response, who must be notified and how fast, who runs your IT.

Audit and Comply
VENDOR COMPLIANCE

Dashboard

Assessments

Vendors

Compliance

Vault

Readiness

Standards

Network

Team

Billing

Notifications

Sipho Dlamini
ADMIN

Sign out

Generate: Access Control & Password Policy

Joiner/mover/leaver access, least privilege, MFA, password rules, and periodic access reviews.

Which systems hold your sensitive data or admin functions?
Microsoft 365, AWS (af-south-1)

Where is multi-factor authentication currently enforced?
M365 only — not yet on AWS

Generate draft

The draft lands in your Company Vault as a draft: read it, edit it, then submit for approval. AI-drafted — not legal advice.

The intake form. Generation runs in the background — refresh the document page in a minute or two.

The AI writes the complete document around *your* answers: your Information Officer by name, your notification windows, containment steps for your actual systems, and honest [insert] placeholders where it lacks facts. It also writes a **first-30-days implementation guide** and suggests the policy's **recurring obligations**.

AI-drafted, human-approved — always. Every generated document lands as a *draft* with a visible banner. It is a strong starting point, not legal advice. You must read it, edit what doesn't fit, and tick an explicit acknowledgement at approval — which is recorded in the immutable audit trail. Fair use: 10 AI drafts per month (Enterprise: uncapped). If drafting fails or you prefer to write it yourself, the document opens with the standard outline instead — never a dead end.

3. Edit, approve, and it becomes evidence

Audit and Comply

VENDOR COMPLIANCE

Dashboard

Assessments

Vendors

Compliance

Vault

Readiness

Standards

Network

Team

Billing

Notifications

Sipho Dlamini

ADMIN

Sign out

Incident Response Plan

← Company Vault · How Acme detects, contains and reports security incidents — including POPIA s 22 notification.

APPROVED

AI-drafted — review every section before approving. This document is a starting point, not legal advice.

Incident Response Plan

Acme AI Inference (Pty) Ltd · Version 1.0 · Owner: Sipho Dlamini, Information Officer

1. Purpose and scope

This plan defines how Acme detects, contains, eradicates and recovers from information-security incidents, and how we meet our notification duties to clients and to the Information Regulator under **POPIA section 22**. It covers all production systems (AWS af-south-1), corporate IT (Microsoft 365), and any incident involving personal information or client business data.

2. What counts as an incident

- Unauthorised access to, or disclosure of, personal information or client data
- Ransomware, destructive malware, or loss of system integrity
- Loss or theft of a device holding company data
- Compromise of credentials, keys or secrets
- Sustained denial of service against production endpoints

3. Roles

Role	Person	Responsibility
Incident Commander	Lerato Mokoena (IT)	Runs the response, owns the timeline
Information Officer	Sipho Dlamini	Regulator and client notification decisions
Communications	Managing Director	Client and public statements
Scribe	On-call engineer	Immutable incident log

4. Response phases and target times

A generated Incident Response Plan: the AI-drafted banner, the rendered policy, the implementation guide, one-click obligation chips, and the lifecycle actions.

- Edit in place** — the built-in editor uses simple markdown; or export to Word, edit there, and upload the file as a new version. Editing an approved policy puts it back into draft for re-approval — content and sign-off always match.
- Approve with acknowledgement** — on approval, a clean Word version files itself into your document library, carrying the right evidence type. That file is what you attach to assessments: "Yes — attached."
- Assessors see the governance.** Wherever the document appears as evidence, reviewers see its state: approved, review current — or review overdue, which is visible pressure to keep things fresh.

4. Obligations: policies that stay true

Audit and Comply

VENDOR COMPLIANCE

Dashboard

Assessments

Vendors

Compliance

Vault

Readiness

Standards

Network

Team

Billing

Notifications

Sipho Dlamini

ADMIN

Sign out

Test the incident response plan

← Incident Response Plan · every 12 months · next due 2026-09-25

Checklist

Was the annual incident resp	Yes/No	☒	evidence
Scenario exercised (e.g. ran	Text	☐	evidence
Were detection and containm	Yes/No	☐	evidence
Was the POPIA s 22 notifica	Yes/No	☐	evidence
Improvement actions raised	Text	☐	evidence
(add a question)	Yes/No	☐	evidence
(add a question)	Yes/No	☐	evidence
(add a question)	Yes/No	☐	evidence
(add a question)	Yes/No	☐	evidence
(add a question)	Yes/No	☐	evidence

An installed obligation: frequency, next due date, a completion checklist (AI-drafted, editable), run history and evidence per run.

Install the suggested obligations (annual plan test, quarterly access review...) with one click, or add your own on any vault document. The platform reminds you at 30 and 7 days, then weekly when overdue. Completing a run means answering the short checklist, attaching evidence (which lands in your library, reusable), and recording the outcome. Findings left open show an amber flag until a remediation update clears them.

5. Review cycles

Set each policy to review every 3/6/12/24 months. When the date nears you'll be reminded; complete the review either as "no changes" or by uploading/writing a new version (which re-enters approval). Overdue reviews are badged everywhere the document appears — including to your assessors — so the pressure to stay current is real but honest.