URAIKKAL

Sample Policy Pack

A worked example of what Uraikkal hands your team — governance categories carried through to a risk-based control matrix, a deployable Netskope policy pack, testing evidence, and the limitations we tell you about up front.

SAMPLE ORGANISATION

Acme Corp

Financial Services · GDPR & HIPAA scope · Netskope GenAI Security & SaaS Protection

179 apps catalogued · 176 fully evaluated · 3 awaiting evaluation

SAMPLE POLICY PACK

Contents

Acme Corp — sample environment

01	**AI Governance**	The governance categories every application is classified into, and how scoped exceptions narrow a category to a specific group without weakening it for everyone else.
02	**Control Matrix**	Risk families × governance categories, with the DLP action chosen for each cell — the decisions your policies enforce.
03	**Netskope Policy Pack**	The recommended policy set in evaluation order, ready to build in-console — not a design document to interpret.
04	**Testing Plan**	Test scenarios mapped to each policy — must-pass and good-to-verify — so "done" has a definition.
05	**Evidence Report**	Captured results per test: expected vs. actual, pass/fail, tester, date — the proof an auditor asks for.
06	**Deployment Checklist**	Every group of objects the pack depends on, tracked to completion — profiles, app objects, identity, notifications, validation.
07	**Limitations & Risks**	What this pack does not cover and why, stated before your architects have to find out the hard way.

This pack is an excerpt — the full engagement covers all risk families, every recommended policy, and every test scenario, not the illustrative subset shown here.

01 · AI GOVERNANCE

Governance categories and scoped exceptions

Acme Corp — sample environment

CATEGORY	WHAT IT MEANS
Prohibited	Blocked outright — access is denied regardless of data type or activity. Used where there is no acceptable business case, or an unmitigated compliance risk.
Restricted / Unassessed	The default for the long tail. An application lands here automatically until it is formally reviewed — access is limited, not blocked, while that review happens.
Approved with Conditions	Allowed, but only for a defined group, data type, or activity. Everything outside those conditions falls back to Restricted / Unassessed.
Approved & Supported	Fully approved for business use, with defined data-handling rules and no restriction beyond the organisation's standard controls.

Scoped groups

Not every policy applies organisation-wide. A scoped policy narrows a governance category to a specific group, business unit, or application instance — in this pack, P210 (Scoped — Corporate Copilot Tenant (Finance)) applies to the Finance group only; every other group still falls under the Restricted / Unassessed fallback for that same application. Scoping is how one governance decision can differ by group without weakening the default for everyone else.

02 · CONTROL MATRIX

Risk families × governance categories

Acme Corp — sample environment

RISK FAMILY	PROHIBITED	RESTRICTED	CONDITIONAL	APPROVED
Credentials, Keys & Secrets	Block	Block	Block	Block
Regulated Data	Block	Block	Coach + Just.	Monitor
Source Code	Block	Coach + Ack.	Monitor	Allow
Intellectual Property	Block	Block	Coach + Just.	Monitor
Security & Infrastructure Data	Block	Coach + Ack.	Monitor	Allow
Customer & Employee Data	Block	Block	Coach + Just.	Monitor
Financial & Commercial Data	Block	Block	Coach + Just.	Monitor
Legal & Contractual Data	Block	Coach + Ack.	Monitor	Allow

Column headers are abbreviated for table width. Official governance categories: Prohibited · Restricted / Unassessed · Approved with Conditions · Approved & Supported.

Excerpt — 8 of 10 risk families shown. Full matrix covers all risk families against all four governance categories.

03 · NETSKOPE POLICY PACK

Recommended policy set, in evaluation order

Acme Corp — sample environment

ID	POLICY NAME	CHANNEL · SCOPE	ACTION
P100	GenAI — Prohibited Applications — Access Block	Web · GenAI	**Block**
P200	GenAI — Secrets & Keys — Global Block	Web · GenAI	**Block**
P210	GenAI — Scoped — Corporate Copilot Tenant (Finance)	Web · GenAI	**Allow**
P295	GenAI — AI Acceptable Use Reminder — Approved & Supported	Web · GenAI	**Coach + Ack.**
P300	GenAI — Approved & Supported — Content Protection	Web · GenAI	**Coach + Just.**
P400	GenAI — Approved with Conditions — Content Protection	Web · GenAI	**Block**
P895	GenAI — AI Acceptable Use Reminder — Catch-all	Web · GenAI	**Coach + Ack.**
P900	GenAI — Restricted / Unassessed — Fallback	Web · GenAI	**Coach + Ack.**

Policies evaluate top to bottom in strict priority order. P100 and P200 are terminal — a match stops evaluation rather than falling through to a lower-priority policy.

URAIKKAL CONTROL INTENT -> NETSKOPE IMPLEMENTATION

Block -> Block

Alert -> Alert

Coach + Acknowledge -> User Alert + notification template

Coach + Justification -> User Alert + justification-required template

Monitor / Allow -> Allow

04 · TESTING PLAN

Scenarios mapped to each policy

Acme Corp — sample environment

35 / 35 must-pass scenarios · 8 / 11 recommended scenarios

TEST	POLICY	SCENARIO	PRIORITY	EXPECTED RESULT
T001	P100	Access a prohibited AI application	**Must-pass**	Block + user coaching shown
T014	P200	Paste an API key into an AI chat prompt	**Must-pass**	Content blocked, alert raised
T027	P300	Submit regulated data via an approved-tier AI app	**Must-pass**	Justification required, then allowed
T031	P400	Submit customer data via a conditionally-approved AI app	**Recommended**	Blocked, incident logged
T038	P900	Access a newly discovered, unassessed AI application	**Must-pass**	Coaching acknowledgement required, access restricted

Excerpt — 5 of 46 scenarios shown.

05 · EVIDENCE REPORT

Captured test results

Acme Corp — sample environment

TEST	EXPECTED	ACTUAL	RESULT	TESTER	DATE
T001	Block + user coaching shown	Matched	**Pass**	R. Alvarez	2026-07-14
T014	Content blocked, alert raised	Matched	**Pass**	R. Alvarez	2026-07-14
T027	Justification required, then allowed	Matched	**Pass**	S. Chen	2026-07-15
T031	Blocked, incident logged	Matched	**Pass**	S. Chen	2026-07-15
T038	Coaching acknowledgement required, access restricted	Matched	**Pass**	R. Alvarez	2026-07-16

Excerpt — 5 of 46 recorded results shown. Full report includes tester notes and screenshots per scenario.

06 · DEPLOYMENT CHECKLIST

What has to exist before the pack goes live

Acme Corp — sample environment

61 / 67 deployment items complete

✓	**Create DLP Profiles**	43/43
✓	**Confirm App Objects**	5/5
✓	**Verify User Identity**	3/3
●	**Notification Templates** 4 remaining: coach templates for 2 new categories, 1 escalation template, 1 executive digest.	8/12
●	**Validation Checks** 2 remaining: SSL inspection re-check, activity support confirmation.	2/4

This is what “deployment-ready” actually means in the deliverable: not a policy list, but every dependency it needs, tracked to completion.

07 · LIMITATIONS & RISKS

Known limitations, and the risk to policy enforcement effectiveness

Acme Corp — sample environment

Stated up front, not discovered later. Each row is a real deployment edge, tracked to an explicit accept/not-yet-accepted decision, not buried in prose.

AREA	LIMITATION	PRACTICAL IMPACT	ACCEPTED
App activity coverage	Not every GenAI app exposes the same real-time activities for DLP inspection.	Some apps may support only partial visibility, so prompt, post, and upload controls may not be consistently enforceable.	Pending
App instance / tenant separation	Enterprise and personal use of the same app may not always be clearly distinguishable.	Personal instances of the same app could be allowed or controlled less accurately.	**Accepted**
AD group dependency	Some apps may not yet have dedicated AD groups defined for user-based scoping.	Until AD groups are established, those apps may need to be handled under Approved with Conditions or Restricted / Unassessed with more restrictive controls.	Pending
User-based allowance risk	Allowing access based only on user identity can create leakage gaps.	Users may bypass the intended corporate-instance-only model by using personal accounts if destination/ instance controls are not reliable.	Pending
Large files / timeout limits	Inline inspection is constrained by file size and scanning limits (default assumption: 128 MB — confirm in tenant).	Large files may cause latency, missed detections, timeout behaviour, or inconsistent enforcement.	Pending

URAIKKAL

From this sample to your own environment.

Everything in this pack — the governance categories, the control matrix, the policy architecture, the evidence — is what Uraikkal produces for your own AI estate, generated the same way for every application you add.

- ✓ Governance decisions that trace directly to a deployable policy, not a slide deck that goes stale
- ✓ Vendor-ready Netskope policies your engineers can build from directly — not a design document to reinterpret
- ✓ One source of truth for auditors, leadership, and engineering, instead of three disconnected documents
- ✓ A repeatable process — every new AI application runs through the same pipeline, not a bespoke review

See this built for your own AI estate.

Request read-only access -> effata.in/contact