

POLICY AND GOVERNANCE

Writing security policies people can actually use

Build a manageable set of security rules, responsibilities and procedures that people can use in their everyday work.

By Haroon Mahmood

A useful security policy helps someone make a decision: how to share a client file, approve a supplier, remove a departing colleague's access or report a mistake. If the reader still has to guess what to do, the document needs more work.

For a growing business, the challenge is often getting a manageable set of rules to work across teams with different priorities. Start with the decisions people face, agree what good practice looks like and make the route easy to follow.

Begin with the situation the policy must improve

Before drafting, write one plain sentence about the problem. For example: "Client information is being shared through several tools, and we cannot reliably tell who still has access." That gives the policy a purpose and helps you judge whether it has made a difference.

Ask the people doing the work to show you the current process. Watch how a project manager shares a document or how IT learns that someone is leaving. Find the delays, missing information and awkward handovers. A rule that depends on information nobody receives will struggle from the start.

This is consistent with the NCSC's advice to develop policies with the workforce and listen to how changes affect their work. [NCSC: Developing a positive cyber security culture](#).

Decide what belongs where

A practical way to organise the material is in three layers:

Layer	What it answers	Example
Policy	What is expected, and who is accountable?	Access to client information must be approved by its business owner.
Standard	What specific conditions apply?	Use named recipients, approved sharing tools and an expiry appropriate to the engagement.
Procedure	How do I do this here?	Open the approved workspace, choose named-recipient sharing and record the approval.

These can be separate documents or clearly labelled sections in one short page. Choose whatever people can find and maintain. Keep frequently changing screen instructions out of a policy that needs senior approval whenever it changes.

Standards provide useful reference points. NIST CSF 2.0 describes policy as something organisations establish, communicate, enforce and update as their circumstances change. It describes outcomes without prescribing a particular document structure. [NIST Cybersecurity Framework 2.0, GV.PO.](#)

Make each rule specific

“Access must be appropriate” leaves several decisions unresolved. Who approves it? Appropriate to which role? Where is the approval recorded? What happens when the project ends?

Use this structure when writing or reviewing a policy:

Element	Question to answer
Purpose and scope	What problem does this address, and which people, information or services does it cover?
Practical rule	What must someone do, avoid or obtain approval for?
Ownership	Who maintains the policy, who performs the activity and who can approve a risk decision?
Procedure	Where are the instructions, approved tools and help route?
Evidence	What existing record shows the rule was followed?
Exceptions	Who can approve a departure, on what terms and until when?
Review	When will the policy be reviewed, and what changes should trigger an earlier review?

An access ticket, approval email in a controlled record or existing service log may provide enough evidence. Choose something the team already produces where possible. A second spreadsheet containing the same information creates another record to keep accurate.

An example: sharing client documents

The following is an illustrative excerpt to adapt to your tools and risks. It is deliberately narrow; it is not a complete information-handling policy.

Scope: *This rule covers client documents shared outside the business.*

Rule: *Staff must use the approved client workspace and share with named recipients. Before sharing, the project owner must confirm that the recipients need the information and approve the*

access end date. Set access to expire on that date or arrange its removal if automatic expiry is unavailable. Public sharing links must not be used for client documents.

How: *Follow the client-workspace sharing instructions. If the recipient cannot use that route, contact the service desk before sending the documents elsewhere.*

Record: *Keep the approval in the project record. The project owner checks external access when the engagement ends and asks IT to remove access that is no longer required.*

Exception: *The designated business risk owner must approve any alternative after security review, recording the reason, safeguards and expiry date.*

Before issuing this, check that the workspace exists, its settings support the rule and somebody will answer the service-desk request. Agree who holds each named role in your organisation. A policy can be clear on paper and still fail at that last step.

Make exceptions useful

Some systems will fall short of a new rule. Record these gaps openly and decide how to handle them before the policy takes effect.

For each exception, capture the affected service, reason, risk, temporary safeguards, accountable owner, approver and expiry or review date. Give recurring exceptions attention: they may reveal a rule that needs revising, a missing capability or an improvement that has repeatedly lost its funding.

Keep the authority clear. The person administering the exception register may not be the person authorised to accept the business exposure. An internal exception also cannot set aside an external obligation; route those cases to whoever owns the relevant contractual or legal requirement.

Test it with a real task

Give the draft to someone who will use it. Ask them to find the answer to a realistic question without explaining it first: “A client wants this file through their own portal. What do you do?”

Listen for hesitation. If they miss the help route, simplify it. If the procedure takes longer than the task allows, work through that constraint with them. Then confirm that managers understand their responsibilities and can apply the rule themselves.

Choose a review interval the owner can sustain, alongside earlier reviews after a relevant incident, system change or repeated exception. NIST’s small-business guide similarly connects governance with clear responsibility, maintained policies and staff understanding. [NIST SP 1300: Small Business Quick-Start Guide](#).

A practical starting point

Take one policy that causes questions today. Before approving its next version, check:

- A reader can explain its purpose and recognise when it applies.
- Each rule names the action and the responsible role.
- The required tools, instructions and support route exist.
- Evidence can be found without recreating the work.
- Exceptions have an approver and an end or review date.
- Someone who performs the task has tried the instructions.
- The owner, approval date and next review are visible.

Experience behind this approach

In previous in-house roles, I aligned enterprise security policies with ISO 27001 and consolidated separate standards into a coherent framework. I also built a software business's information security management system, including its policies, standards and operating processes. That experience informs my approach at Kurosec: connect the written requirement to the team, process and evidence needed to make it work.

Kurosec's [security policies and governance service](#) can help you simplify existing documents or build a practical set around your business. [Contact us](#) to discuss where your team is getting stuck.

Further reading

- [NIST Cybersecurity Framework 2.0](#) - policy outcomes in the Govern function.
- [NCSC: Developing a positive cyber security culture](#) - involving people in policy and process design.
- [NIST Small Business Quick-Start Guide](#) - a starting point for security responsibilities and priorities.