Security Policy Development Worksheet

Plan one security policy and the procedure, responsibilities and records needed to support it.

How to use these four pages

1. Choose an activity, its purpose and the people who need guidance.

2. Separate the management expectation, operating steps and evidence record.

3. Use a fictional walkthrough to identify unclear responsibilities.

4. Agree approval, communication and review before introducing the controlled version.

A practical working aid

Use the blank records for your own discussion. Examples are fictional, not client case studies. Print to complete by hand or adapt the prompts in your own document; this PDF is not a fillable form.

Keep completed records confidential. Use references to protected evidence rather than passwords, customer records or sensitive system details.

Online instructions and companion article

Read the guide

Read the article

Source guidance

NIST Cybersecurity Framework (CSF) 2.0

Public guidance checked 10 November 2026. The source material informs the approach; no endorsement is implied. This worksheet supports planning and record-keeping. It does not authorise testing, certify compliance or replace an agreed specialist review.

Free to use and adapt within your business with the GRCPreneur acknowledgement retained.

A fictional worked example

Illustrative entries only. No real client, vendor result or completed implementation is claimed.

Record	Illustrative entry
Purpose	Make supplier-access requests and completion checks understandable.
Policy expectation	Supplier access requires approval for a defined business purpose.
Procedure roles	Sponsor requests; owner approves; administrator carries out agreed changes.
Evidence record	Protected approval and closure references, including exceptions.
Walkthrough finding	No person initially owned the final check; the draft assigns that role.
Next decision	Approver reviews the revised document and communication plan.

Before using the blank pages

Agree who will review the record and what decision it supports. Mark assumptions, proposed actions and unverified claims clearly. Copy pages 3 and 4 when you need more space.

Your working record

Project / record ID: _____ Date: _____

Purpose, scope and audience

What activity needs a rule? Who needs to understand and apply it?

Expectation and requirements

State the rule and sources. Mark applicability questions for confirmation.

Operating steps and responsibilities

Trigger, request, approval, performance, check and supplier handover.

Exceptions and evidence

Escalation, exception authority, ending conditions and protected records.

Approval, introduction and review

Owner, approver, version, walkthrough, communication and review triggers.

Use protected evidence references. Do not enter credentials or confidential customer details.

Policy decisions and implementation

Related record / requirement: _____ Review date: _____

Decision / improvement	Evidence / completion check	Owner / due date	Approval / next review

Review before the next decision

- Expectation, operating steps and evidence have distinct purposes.
- Roles and exception routes can be understood by intended users.
- Approval, controlled version and communication are planned.
- Review triggers and evidence of use have owners.

Decision, authority and next checkpoint

Proceed / revise / defer / stop. State the decision scope, conditions, approver and date.

A completed record documents a review. Approval applies only to the stated scope and does not establish that untested work has succeeded.