APEX

DOCUMENTATION GROUP

Sample Work Portfolio.

Representative deliverables: SOP rewrites, policy development, knowledge-base structure, documentation audits, and governance.

DOCUMENTATION, GOVERNANCE & COMPLIANCE

ABOUT THESE SAMPLES

All samples were prepared for "Summit Manufacturing," a fictional company, to demonstrate structure, standards, and quality of work. Client engagements are confidential; deliverables are never shared without written permission.

ApexDocumentationGroup.com · hello@apexdocumentationgroup.com

Before & After: SOP Rewrite

The same procedure — before and after an Apex Documentation Rescue Sprint.

BEFORE

SOP: User Access

This procedure outlines the steps required to provision user access in the system.

1. Submit request
2. Get approval
3. Create account
4. Notify user
5. Update spreadsheet

- ✗ No document ID or version
- ✗ No owner or approver
- ✗ No timing, systems, or exceptions
- ✗ No related documents
- ✗ Last updated: unknown

AFTER

SOP-IT-004 · User Access Provisioning

v2.0 · Effective 03/2026 · Review 03/2027 · Owner: IT Security

1.0 PURPOSE
Define the standard, auditable process for granting system access.

2.0 SCOPE
All access requests for internal users and contractors.

3.0 STEPS
Role-based table: action, owner, system, SLA, evidence.

4.0 EXCEPTIONS
Emergency access path with required post-approval.

5.0 REFERENCES
Access Policy POL-SEC-002, request form, audit log.

- ✓ Versioned, owned, and approval-tracked
- ✓ Every step has an owner and an SLA

WHAT CHANGED

Ambiguous steps became a structured, role-based procedure with ownership, timing, exceptions, and references — the difference between a document that describes work and one that survives an audit.

Structure
Consistent sections and layouts make documents easy to create, read, and maintain.

Ownership
Every document carries an owner, approver, and review date — accountability built in.

Evidence
Steps map to audit evidence, so proof is generated as the work happens.

Standard Operating Procedure

Full sample deliverable — User Access Provisioning (fictional client).

OWNER	EFFECTIVE	REVIEW DUE	STATUS
IT Security	03/01/2026	03/01/2027	Approved

1.0 PURPOSE

To define the standard process for provisioning user access to Summit Manufacturing systems in a secure, consistent, and auditable manner, ensuring access is granted only with documented approval.

2.0 SCOPE

Applies to all system access requests for internal employees and contractors. Excludes third-party vendor access, which is governed by SOP-IT-007.

3.0 PROCEDURE

STEP	ACTION	OWNER	SLA	EVIDENCE
1	Submit access request via IT portal	Requestor	—	Ticket ID
2	Verify role and access level against matrix	IT Access Analyst	4 bus. hrs	Matrix check noted in ticket
3	Approve or reject request	System Owner	1 bus. day	Approval recorded in ticket
4	Provision account with least privilege	IT Access Analyst	4 bus. hrs	System log entry
5	Notify requestor; confirm first login	IT Access Analyst	1 bus. day	Closure note
6	Log completion in access register	IT Access Analyst	Same day	Register entry

4.0 EXCEPTIONS

Emergency access may be granted verbally by the System Owner and must be documented in the access register within one business day, with retroactive approval attached to the ticket.

5.0 RELATED DOCUMENTS

POL-SEC-002 Access Control Policy · FRM-IT-011 Access Request Form · Access Control Matrix · Quarterly Access Review Checklist

APPROVED BY	DATE	DOCUMENT CONTROL
J. Rivera, Director of IT (fictional)	02/24/2026	Quality & Compliance

Information Security Policy

Full sample deliverable — policy structure and language (fictional client).

OWNER	APPROVER	EFFECTIVE	REVIEW
Information Security	VP, Operations	03/01/2026	Annual

1.0 PURPOSE

To establish the requirements for protecting Summit Manufacturing's information assets against unauthorized access, disclosure, alteration, or loss.

2.0 SCOPE

Applies to all employees, contractors, systems, and data owned or operated by the company, in all locations and work arrangements.

3.0 POLICY STATEMENT

Summit Manufacturing is committed to maintaining the confidentiality, integrity, and availability of its information. Access to information is granted on the principle of least privilege and revoked promptly when no longer required.

4.0 POLICY REQUIREMENTS

4.1 All system access must be requested, approved, and provisioned per SOP-IT-004.

4.2 User access rights are reviewed quarterly by system owners; results are documented.

4.3 Company data is classified as Public, Internal, or Confidential, and handled per its classification.

4.4 Security incidents must be reported to Information Security within 24 hours of discovery.

4.5 Exceptions to this policy require written approval from the policy owner and are time-limited.

5.0 ROLES & RESPONSIBILITIES

ROLE	RESPONSIBILITY
Information Security	Maintains this policy; monitors compliance; leads incident response
System Owners	Approve access; conduct quarterly access reviews
All Users	Follow policy requirements; report incidents promptly
Document Control	Maintains versioning, approvals, and the annual review cycle

6.0 EXCEPTIONS & ENFORCEMENT

Exceptions are logged in the policy exception register with expiry dates. Violations may result in access revocation and disciplinary action consistent with company procedures.

Knowledge Base: Structure & Article

Sample taxonomy plus a rewritten self-service article (fictional client).

KNOWLEDGE BASE TAXONOMY

- ► Getting Started
- ► Policies & Standards
- ► **Processes & Procedures**
  - Access Management
  - Incident Management
  - Change Management
  - Vendor Management
- ► Forms & Templates
- ► Systems & Tools
- ► Training & Resources
- ► FAQs
- ► Change Log

How to Request Software Access

Processes & Procedures › Access Management · Updated 03/2026 · 2 min read

OVERVIEW

Use this process to request access to any company system. Most requests are completed within one business day.

STEPS

1. Open the IT portal and select “Request Access.”
2. Choose the system and the role you need.
3. Add a one-line business reason.
4. Submit — your manager and the system owner approve.
5. You'll get an email when access is ready.

GOOD TO KNOW

Access is role-based: if a teammate in the same role has it, your request is usually pre-approved. Emergency access? See the exception process in SOP-IT-004.

Related: Access Control Policy · New Hire Onboarding · Tags: access, IT, onboarding

WHY THIS WORKS

One topic per article, a scannable structure, plain language, and consistent categorization — so employees find answers in seconds instead of re-asking the same questions.

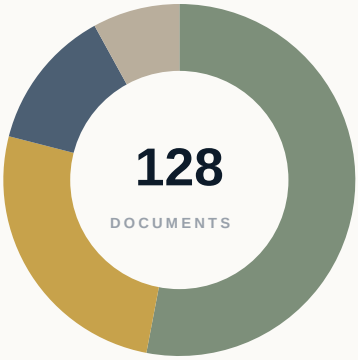
Findability
Taxonomy and tags mirror how the team actually searches, not how files were saved.

Trust
Version dates and owners on every article — people rely on what they find.

Self-service
Fewer repeat questions to managers, IT, and HR; faster onboarding.

Documentation Audit: Executive Summary

Sample audit output — portfolio health assessment across 128 documents (fictional client).



Compliant	68 docs (53%)
Needs update	33 docs (26%)
Major gaps	17 docs (13%)
Obsolete	10 docs (8%)

47% of the portfolio requires action before the next audit cycle.

TOP FINDINGS

#	FINDING	RISK	RECOMMENDED ACTION
1	Inconsistent naming conventions across departments	Medium	Adopt portfolio-wide naming standard
2	41 documents missing an owner or approver	High	Assign ownership via governance matrix
3	Outdated content referencing retired systems	High	Rewrite in priority order (see roadmap)
4	No version control on shared-drive documents	Medium	Introduce version blocks + change log
5	Gaps in audit-evidence trail for key processes	High	Add evidence columns to core SOPs

WHAT THE CLIENT RECEIVES

The full audit includes a per-document scorecard (accuracy, clarity, completeness, consistency, compliance, accessibility, ownership, version control), a prioritized remediation list, and the 30-day roadmap on the following page.

Prioritized
Findings ranked by risk so effort goes where exposure is highest.

Measurable
A baseline health score to track improvement quarter over quarter.

Actionable
Every finding pairs with a concrete, owner-assigned recommendation.

Governance Matrix & 30-Day Roadmap

Sample governance structure and the improvement plan delivered with every Rescue Sprint.

DOCUMENT GOVERNANCE MATRIX (EXCERPT)

PROCESS AREA	POLICY OWNER	PROCESS OWNER	REVIEW	RISK
Access Management	IT Security	IT Operations	Annual	High
Change Management	IT Governance	Change Manager	Bi-annual	Medium
Incident Management	IT Security	Service Desk	Quarterly	High
Vendor Management	Procurement	Vendor Manager	Annual	Medium
Document Control	Quality	QA Manager	Annual	Low

30-DAY DOCUMENTATION ROADMAP

WEEK 1

Discover & Align

- Kickoff and alignment
- identify critical documents
- audit existing content
- define priorities

WEEK 2

Build & Draft

- Draft key documents
- build templates
- structure the knowledge base
- gather stakeholder input

WEEK 3

Review & Revise

- Review and edit
- validate accuracy
- check compliance
- refine and approve

WEEK 4

Finalize & Launch

- Publish
- train the team
- set the review cadence
- plan the next 30 days

SUCCESS METRICS

Adoption by the team · accuracy of rewritten content · compliance coverage · time-to-find for key documents. Clear steps. Measurable progress. Confident results.

Ready to see your documentation at this standard?

The Documentation Rescue Sprint delivers this structure for your three highest-priority documents in 7 business days. Starting at $2,000.

SCHEDULE A DOCUMENTATION RESCUE CALL

ApexDocumentationGroup.com · hello@apexdocumentationgroup.com

DOCUMENTATION, GOVERNANCE & COMPLIANCE