CLOUDSWITCHED

FREE RESOURCE — DOCUMENTATION TEMPLATE

Network Documentation Template

Document your network topology, IP addressing, VLANs, hardware, WAN links, DNS and access controls in a structured, maintainable format. Essential for troubleshooting, compliance, knowledge transfer and onboarding a new MSP — fillable in any modern PDF viewer.

7	70+	A4	Fillable
DOCUMENTATION SECTIONS	INVENTORY & CONFIG FIELDS	PRINT & RUNBOOK READY	TYPE & TICK IN ANY VIEWER

IP & VLAN · HARDWARE & FIRMWARE · WAN & DNS · ACCESS CONTROL

PREPARED FOR	PREPARED BY	VERSION	FORMAT
Cloudswitched Knowledge Library	Cloudswitched Ltd.	2026 Edition	Living Document

00

How to use this template

Complete each of the seven sections to build a comprehensive documentation pack for your network. Capture **what is actually deployed today** — not what was specified two years ago and is now drifting. Fill the inventory tables (subnets, VLANs, hardware, DNS records) using your live configuration, not your runbook.

This is a **living document**. Store it securely (encrypted, access-controlled) and update it after every change — new firewall rule, new VLAN, new access point, new public IP. Schedule a quarterly review so accuracy never drifts. The yellow underscore lines become real text inputs in any modern PDF viewer; the squares become real checkboxes.

WHAT THIS TEMPLATE IS

A structured snapshot of your network topology, addressing, segmentation, hardware estate, WAN links, DNS / DHCP services and access controls. It is the artefact your IT team, a new MSP, an auditor or an incident responder will need on day one. Pair it with our network infrastructure assessment and network security audit checklist for a full review cycle.

SECURITY WARNING

Do **not** store device passwords inline in this document. Reference the password manager vault and entry name only (Section 07). All network device credentials should live in an approved password manager (1Password, Keeper, Bitwarden, Azure Key Vault) with MFA-protected access and a documented break-glass procedure.

The seven sections

- **01 Network Overview & Diagram** — topology summary, sites, users, diagram reference.
- **02 IP Address Management** — subnets, CIDR ranges, gateways, DHCP scopes, static allocations.
- **03 VLAN Configuration** — segmentation, tagging, trunks, access ports, ACL rules.
- **04 Hardware Inventory & Configuration** — firewalls, switches, APs, firmware, support expiry, backup.
- **05 Internet & WAN Links** — primary, backup, site-to-site VPN, circuit references, costs.
- **06 DNS & DHCP Configuration** — internal DNS, forwarders, key external records, domain.
- **07 Credentials & Access** — password manager reference, access restrictions, sign-off.

01

Network Overview & Diagram

Capture the high-level summary of the network estate and reference the live topology diagram. The diagram is the source of truth for shape; this page is the source of truth for **who owns it, when it was last touched and where the diagram lives**.

DOCUMENT METADATA

Organisation	
Documentation version	
Last updated *(DD/MM/YYYY)*	
Updated by	
Next review due	

ESTATE SUMMARY

Total sites	
Total users	
Total endpoints *(laptops / desktops / mobile)*	
Primary IT contact	
Out-of-hours contact	

DIAGRAM REFERENCE

Network diagram location *(file path / URL)*	
Diagram tool *(draw.io / Visio / Lucidchart)*	
Editable source file kept with this doc	☐ Yes ☐ No
Separate logical & physical diagrams	☐ Yes ☐ No ☐ N/A

DIAGRAM BEST PRACTICES

Use a consistent colour scheme: **blue** for switches, **red** for firewalls, **green** for servers, **orange** for wireless. Include IP addresses, interface names and link speeds on the diagram itself. For complex multi-site environments, maintain separate logical (L3) and physical (cabling/rack) diagrams.

02

IP Address Management (IPAM)

Document every subnet in use, the VLAN it lives on, the gateway address and the DHCP scope. Static IP allocations (servers, printers, APs, appliances) are listed separately so they survive a DHCP rebuild without anybody guessing.

SUBNETS & DHCP SCOPES

SUBNET	CIDR	VLAN	GATEWAY	DHCP RANGE	DESCRIPTION
192.168.1.0	/24	VLAN 1	192.168.1.1	.100–.200	Corporate LAN
10.0.10.0	/24	VLAN 10	10.0.10.1	Static only	Server infrastructure
10.0.20.0	/24	VLAN 20	10.0.20.1	.100–.200	VoIP phones
10.0.30.0	/24	VLAN 30	10.0.30.1	.50–.200	Wireless clients
10.0.99.0	/24	VLAN 99	10.0.99.1	.50–.150	Guest WiFi (isolated)
_____	_____	_____	_____	_____	_____
_____	_____	_____	_____	_____	_____

STATIC IP ALLOCATIONS

IP ADDRESS	HOSTNAME	DEVICE TYPE	LOCATION	NOTES
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____

EXAMPLE ROWS ARE TEMPLATES, NOT CONSTRAINTS

The first five subnet rows show a common UK SME pattern (corporate, servers, VoIP, wireless, guest). Overwrite or extend as needed. The blank static-IP rows take any device that must hold a fixed address — printers, NAS, hypervisors, APs, security appliances, IoT controllers.

03

VLAN Configuration

Document every VLAN in use, its subnet, the trunk and access ports that carry it and any ACL rules that segregate traffic. A clear segmentation map is the foundation of every later security control — firewall zones, NAC policy, IoT isolation.

VLAN ID	NAME	SUBNET	TRUNK PORTS	ACCESS PORTS	ACL RULES	PURPOSE
1	**Default**	192.168.1.0/24	All trunks	Unassigned	Full access	Legacy / management
10	**Servers**	10.0.10.0/24	All trunks	Server ports	Block from guest	Server infrastructure
20	**VoIP**	10.0.20.0/24	All trunks	Phone ports	QoS priority	IP telephony
30	**Wireless**	10.0.30.0/24	AP trunks	N/A	Standard access	Wireless clients
99	**Guest**	10.0.99.0/24	AP trunks	N/A	Internet only	Guest access

INTER-VLAN ROUTING & SEGMENTATION

Routing performed by *(firewall / L3 switch)* _____

Inter-VLAN ACLs enforced ☐ Yes ☐ No ☐ Partial

Guest VLAN fully isolated from corporate ☐ Yes ☐ No

WHAT GOOD LOOKS LIKE

A VLAN-to-port mapping kept on the comms rack — not in someone's head. Trunks documented end-to-end. Native VLAN explicitly set (not VLAN 1 by default). Voice and data VLANs separate. Guest and IoT VLANs default-deny back to corporate, internet-only.

04

Hardware Inventory & Configuration

Document every network device, its model, firmware, serial number and the date support ends. Without firmware and support-expiry dates captured here, vulnerability management and budgeting both drift into guesswork.

HOSTNAME	TYPE	MAKE / MODEL	SERIAL	LOCATION	IP ADDRESS	FIRMWARE	SUPPO EXPIR
_____	Firewall	_____	_____	_____	_____	_____	_____
_____	Core switch	_____	_____	_____	_____	_____	_____
_____	Access switch	_____	_____	_____	_____	_____	_____
_____	Access point	_____	_____	_____	_____	_____	_____
_____	_____	_____	_____	_____	_____	_____	_____
_____	_____	_____	_____	_____	_____	_____	_____

CONFIGURATION BACKUP

Backup location *(server / cloud / vault)* _____

Backup frequency _____

Backup method *(automated / scripted / manual)* _____

Last successful restore test _____

Off-site copy retained ☐ Yes ☐ No

SUPPORT EXPIRY IS A HARD CEILING

Network kit running past its vendor support date stops receiving security patches and is uninsurable under most cyber policies. Treat the support-expiry column as a budget trigger, not an aspiration. A documented refresh schedule beats a panic replacement after a CVE.

05

Internet & WAN Links

Document every internet circuit, backup link and site-to-site VPN that terminates on site. Capture circuit references and contract end dates — without these, fault tickets stall at the ISP and renewals get missed.

CIRCUIT	ISP	TYPE	BANDWIDTH	IP RANGE	CIRCUIT REF	MONTHLY £	C E
Primary							
Backup							
Site-to-Site VPN							

FAILOVER & RESILIENCE

Failover method *(automatic / manual / none)* _____

Failover tested in last 12 months ☐ Yes ☐ No

Public IP block portable to new address ☐ Yes ☐ No ☐ Unknown

ISP technical support number _____

LEAD TIMES

Leased lines routinely take **60–90 business days** for delivery and cross-connects. Order new circuits 8 weeks before any office-move target date and confirm with the ISP whether the public IP block, CPE and SIP DDIs transfer with the service or require re-provisioning.

06

DNS & DHCP Configuration

Document the internal DNS servers, external forwarders, the public domain and the key external records mail and web services depend on. A missing SPF or MX entry is a five-minute fault that takes hours to diagnose without this page.

DNS CONFIGURATION

Primary internal DNS server _____

Secondary internal DNS server _____

External forwarders *(e.g. 1.1.1.1, 8.8.8.8)* _____

Internal domain name _____

External / public domain _____

DNS hosted by *(Cloudflare / Route 53 / registrar)* _____

DNSSEC enabled on external zone ☐ Yes ☐ No

KEY EXTERNAL DNS RECORDS

RECORD TYPE	HOSTNAME	VALUE	TTL	PURPOSE
A	_____	_____	_____	_____
MX	_____	_____	_____	_____
TXT (SPF)	_____	_____	_____	_____
TXT (DKIM)	_____	_____	_____	_____
TXT (DMARC)	_____	_____	_____	_____
CNAME	_____	_____	_____	_____

SPF, DKIM, DMARC ARE MANDATORY

Major mailbox providers (Microsoft, Google, Yahoo) now reject or quarantine bulk mail from domains without a valid SPF, aligned DKIM signature and a published DMARC policy. Document the current records here and tighten DMARC from p=none to p=quarantine or p=reject on a planned cadence.

07

Credentials & Access

Reference — **do not store inline** — the secure location of all network device credentials. Capture the vault, the entry naming convention and who is authorised to break the glass.

SECURITY WARNING

Do **NOT** store passwords in this document. Reference the password manager vault and entry name only. All network device credentials should live in an approved password manager (1Password, Keeper, Bitwarden, Azure Key Vault) with MFA-protected access and an audited break-glass procedure.

PASSWORD MANAGER REFERENCE

Password manager used	_____
Vault name	_____
Entry naming convention	_____
Access restricted to *(group / role)*	_____
MFA enforced on vault	☐ Yes ☐ No
Break-glass procedure documented	☐ Yes ☐ No

ADMIN ACCOUNTS & STORAGE

DEVICE / SYSTEM	ADMIN ACCOUNT LABEL	VAULT ENTRY REFERENCE	MFA	LAST ROTATED
Firewall	_____	_____	_____	_____
Core switch	_____	_____	_____	_____
Wireless controller	_____	_____	_____	_____
ISP portal	_____	_____	_____	_____
DNS provider	_____	_____	_____	_____
Backup / NAS	_____	_____	_____	_____

08

Review & Sign-off

This is a living document. Capture the top three actions that came out of this review cycle, any notes that don't fit elsewhere, and the names of the people approving the snapshot. Re-walk the seven sections each quarter and after every material change.

Top 3 priority actions

01 _____

02 _____

03 _____

Additional notes

_____

_____

_____

_____

Sign-off

PREPARED BY	DATE	APPROVED BY
_____	_____	_____

CLOUDSWITCHED

NETWORK DOCUMENTATION & IT OPERATIONS

info@cloudswitched.com

New London House, 6 London St
London EC3R 7LP · United Kingdom