CLOSE PHASE · TEMPLATE

Decommission checklist

Removes the old environment safely after migration: retention and backup checks first, then data, accounts, licences, DNS and hardware, with evidence and sign-off.

CM-TPL-CLS-02 · v1.0 · November 2026

Latest version

PROJECT	OWNER	STATUS	LAST UPDATED
[Project name]	[Name, role]	Draft	[YYYY-MM-DD]

How to use this template

1. Do not start until hypercare is closed and the business owner has confirmed the old environment is no longer used.
2. Complete the retention and backup sections first. Nothing is deleted until both are signed.
3. Record evidence for each item (report, screenshot, ticket number); auditors and legal will ask.
4. Work through the sections in order: data and access first, then licences, then DNS and hardware.
5. Note licence renewal and notice dates early so you cancel before the next term starts.

1. Scope and readiness

List what is being decommissioned and confirm the preconditions.

- Hypercare closed and signed off.
- Business owner confirms in writing that the old environment is no longer needed.
- Usage reports show no sign-ins or file activity for at least 30 days (except service accounts on the exception list).
- Rollback plan formally retired by the sponsor.

SYSTEM OR ENVIRONMENT	OWNER	REPLACED BY	LAST USED DATE	PLANNED REMOVAL DATE
Fabrikam Microsoft 365 tenant		Contoso tenant		
FAB-FS01 file server		SharePoint Online		
Legacy mail filtering service		Exchange Online Protection		

2. Retention and legal checks (before any deletion)

Confirm with records management or legal. Australian organisations commonly keep financial records for 5 to 7 years; government agencies follow their records authority. Write the actual rule here.

CHECK	EVIDENCE	OWNER	DONE
Records retention requirements confirmed for each data type (email, finance, HR, contracts)	Records manager email		
No litigation holds or eDiscovery cases active on source mailboxes or sites	Purview eDiscovery and hold report		
Retention policies in source reviewed; equivalent policies active in target	Policy comparison		

General information only, not professional advice. © 2026 Cloud-Migrations.au · cloud-migrations.au/templates

CHECK	EVIDENCE	OWNER	DONE
Decision recorded for leavers and inactive mailboxes (migrate, export or keep as inactive)	Decision log		
Audit logs exported if they must be kept longer than the platform keeps them	Export location		
Privacy obligations met for personal information being destroyed	Privacy officer confirmation		

3. Backup and final export checks

Assume you will need something after it is gone. Prove you can get it back.

CHECK	EVIDENCE	OWNER	DONE
Final full backup or export taken of mailboxes, OneDrive, SharePoint and file shares	Backup job report		
Test restore of a sample mailbox, site and folder from the final backup	Restore test record		
Backup retention period matches the retention requirement	Backup policy		
Export location secured, encrypted and access restricted	Access list		
Migration reconciliation reports archived with the project	Project site link		

4. Data

Remove data only after the two sections above are complete.

ITEM	ACTION	EVIDENCE	OWNER	DONE
Source mailboxes	Remove licences; mailboxes enter soft-delete, then purge after the retention window	Mailbox report		
Source OneDrive accounts	Confirm retention setting for deleted users; then remove	Admin report		
Source SharePoint sites and Teams	Delete after read-only period; empty site recycle bins only when approved	Site list		
File server shares	Set read-only, then offline for 30 days before wiping	Change record		
Virtual machines	Power off for a holding period, take final backup, then delete VMs and storage	Hypervisor report		
Snapshots, replicas and old backups	Remove those no longer covered by retention	Storage report		

5. Accounts and identity

Include non-human accounts; these are often missed.

ITEM	ACTION	EVIDENCE	OWNER	DONE
User accounts in source	Delete after data and licence steps	User count report		

General information only, not professional advice. © 2026 Cloud-Migrations.au · cloud-migrations.au/templates

ITEM	ACTION	EVIDENCE	OWNER	DONE
Admin and break-glass accounts	Disable last; record date	Admin role report		
Service accounts	Identify dependants; disable, wait, then delete	Service account list		
App registrations and enterprise apps	Remove from source; confirm replacements in target	App list		
Entra Connect / directory sync	Disable sync in tenant, uninstall server, remove sync account	Change record		
Guest accounts and external sharing links	Review and remove	Guest report		
Shared credentials in password vault	Archive or delete entries for the old environment	Vault audit		

6. Licences and subscriptions

Record dates and notice periods, not amounts. Check auto-renewal settings.

LICENCE OR SUBSCRIPTION	RENEWAL DATE	NOTICE PERIOD	ACTION	OWNER	DONE
Microsoft 365 licences (source tenant)			Reduce to zero, then cancel		
Migration tool licences			Confirm no re-runs needed; cancel		
Third-party backup for source tenant			Keep until retention ends or export		
Mail filtering / archiving service			Cancel after MX moved and archive exported		
Hardware and software maintenance contracts			End or transfer		

7. DNS, network and certificates

Remove stale records so they cannot be hijacked or confuse clients.

ITEM	ACTION	EVIDENCE	OWNER	DONE
Old verification TXT records (MS=..., google-site-verification)	Remove	Zone export		
Records pointing to decommissioned hosts	Remove to prevent subdomain takeover	Zone review		
SPF includes for retired services	Remove	SPF lookup		
TTLs lowered for cutover	Return to normal values	Lookup		
Firewall rules, NAT, VPN tunnels and connectors	Remove	Firewall change record		

General information only, not professional advice. © 2026 Cloud-Migrations.au · cloud-migrations.au/templates

ITEM	ACTION	EVIDENCE	OWNER	DONE
Certificates for old hosts	Revoke or let expire; remove renewal reminders	Certificate inventory		
Unused domains	Decide: keep (brand protection) or let lapse	Domain register		

8. Integrations and third parties

Anything that sent mail, synced data or authenticated against the old environment.

- SMTP relays from scanners, applications and line-of-business systems moved and old connectors removed.
- Single sign-on apps moved to target identity provider.
- Vendors and partners told of new contacts and addresses.
- Monitoring checks for the old environment removed so they do not raise false alerts.
- CMDB and asset register updated to show items as retired.

9. Hardware disposal

Use an accredited disposal provider and keep certificates. Government agencies follow ISM media sanitisation guidance.

ASSET	SERIAL / TAG	SANITISATION METHOD	CERTIFICATE REF	DONE
FAB-FS01 file server		Disk wipe and certified destruction		
Storage array				

10. Sign-off

Retention and backup sign-off is required before data deletion. Final sign-off after all sections are complete.

STAGE	ROLE	NAME	SIGNATURE	DATE
Retention and backup checks complete	Records manager / legal			
Retention and backup checks complete	IT operations manager			
Decommission complete	Business owner			
Decommission complete	Project manager			

Approval

NAME	ROLE	SIGNATURE	DATE

CM-TPL-CLS-02

General information only, not professional, legal or technical advice. Adapt this template to your organisation, test procedures in a non-production environment and keep verified backups. To the extent permitted by law, Cloud-Migrations.au accepts no liability for loss arising from its use. © 2026 Cloud-Migrations.au. Free to use and adapt within your organisation.