PH7X SYSTEMS ®

0.3.0 · CHAPTER 39

Hand over every control with an owner, a reading and a review date

SharePoint Migration Field Guide · Chapter 39

pH7x Systems

2026-11-07

39. Hand over every control with an owner, a reading and a review date

> The project sets every control once. Everybody who changes one afterwards was never in the project.

Chapter 6 wrote the destination's rules before the first wave and gave each an owner. Chapter 9 closed every wave and set the evidence gate for decommissioning the source. This chapter takes the day after, when the team leaves and its settings stay with whoever administers them next.

> **Which controls must hold on the destination from the day the project closes, and who owns each one after the migration team leaves?**

The decision this chapter leads to is a list of controls, each with its owner, a documented way to read its state and a review date, signed before the project closes.

Which destinations this chapter is for

A SharePoint Online tenant that received sites by copy (Chapters 8, 9 and 24), and a Subscription Edition farm that received them by attach (Chapter 23). A hybrid estate keeps both lists, plus Chapter 25's features and their exit dates.

Close the project's own access first

A migration needs more access than operation does. SPMT needs a SharePoint Administrator or Global Administrator to migrate at organisation level, or a site admin of each site collection; Microsoft recommends roles "with the fewest permissions" and keeps Global Administrator for "emergency scenarios" (install SPMT). A migration app limited to selected sites needs FullControl on every destination site before it starts (certificate-based migration, both checked on 7 November 2026). Nothing in the migration removes that access.

We would close the project's access before anything else: its accounts leave every role and site they joined, its app loses its grants and is deleted or given an owner, and the identity team reads the assignments again with `Get-MgRoleManagementDirectoryRoleAssignment` (role assignments, checked on 7 November 2026).

On a farm, members of a server's local Administrators group "can perform all farm administrator actions" (administration hierarchy), so the project leaves that group on every server, the Farm Administrators group and every web application's user policy. Microsoft names an administrator

leaving as a reason to reset all service account passwords at once (automatic password change, both checked on 7 November 2026). We would reset every password the project knew on the day it closes.

The controls on SharePoint Online

CONTROL	WHERE IT IS SET	HOW ITS STATE IS READ	OWNER AFTER THE PROJECT
External sharing and default links	Admin centre, Policies > Sharing; each site's own setting	That page; `Get-SPOSite -Identity`, one site at a time	SharePoint service owner
Who creates sites and groups	Admin centre, Settings > Site creation; the `Group.Unified` directory setting	That page; `Get-MgBetaDirectorySetting` and its `Values`	SharePoint service owner; identity team for groups
Group naming and expiration	Entra admin centre, Groups: Naming policy, Expiration	The same `Values`; `Get-MgGroupLifecyclePolicy`	Identity team
Inactive and ownerless sites	Site lifecycle management policies; the ownerless group policy	Each policy's execution report; the Ownerless groups filter	SharePoint service owner, with site owners
Retention and sensitivity labels	Purview policies and labels; each site's label	`Get-RetentionCompliancePolicy -DistributionDetail`; the site's `SensitivityLabel`	Records owner; information protection owner
Admin roles	Entra roles	`Get-MgRoleManagementDirectoryRoleAssignment`	Identity team
Audit log	Purview Audit; retention by licence and policy	`Get-AdminAuditLogConfig` in Exchange Online PowerShell; `Get-UnifiedAuditLogRetentionPolicy`	Security or compliance owner
Service changes	Message centre	Its posts, saved with ID and date before they expire (Chapter 41)	The reader Chapter 24 named

Sources: sharing, Get-SPOSite, site creation, group creation, naming, expiration, inactive sites, ownership, ownerless groups, container labels, retention policies, audit retention and turning audit on, all checked on 7 November 2026. The owners are our suggestion; the record names a person.

Sharing is read one site at a time. A site's sharing can match the organisation's or be stricter, never wider (sharing, above), and `Get-SPOSite` called with `-Limit` or `-Filter` leaves each site's sharing properties and label unpopulated, where they "may contain a default value" (Get-SPOSite, above). Labels move part of this control: once a label's sharing settings are published, "a site owner can now set and change these options" by changing the label (container labels, above), so whoever owns the labels owns that part of sharing.

Creation and expiry live in the directory. Turning off site creation leaves users able to create Microsoft 365 groups, and each group "always comes with a team site" (site creation, above). Microsoft calls letting everyone create groups "the recommended approach" (group creation, above), so a restriction is your convention, with its reason. The naming policy applies to groups users create and exempts Global Administrators and User Administrators (naming, above). An expiration policy renews active groups, warns owners 30, 15 and 1 days ahead, and deletes the rest with their sites, restorable for 30 days (expiration, above). An archived group-connected site leaves the rest of its group active (archive management, checked on 7 November 2026), and we do not know whether expiry spares it. We would put a group kept for an obligation, like Chapter 27's archives, under expiration only with its records owner's agreement.

Lifecycle policies notify; owners decide. The inactive site and site ownership policies run monthly in active mode; after three monthly notifications they do nothing, set the site read-only, or archive it after 3, 6, 9 or 12 months read-only, and a certified site goes unchecked for a year (inactive sites, above). Their scope includes sites locked read-only for other reasons, Chapter 26's among them (same source). Ownership enforcement acts only on sites with no owner (ownership, above). Activity counts views, edits, shares and syncs, with Teams, Exchange and Viva Engage, never app tokens (inactive sites, above): a new measure, not a continuation of Chapter 14's. Both are SharePoint Advanced Management features, tied to certain licences, the Plan 1 add-on among them (prerequisites, checked on 7 November 2026). The ownerless group policy asks active members weekly and, if nobody accepts, "takes no further action" (ownerless groups, above): somebody has to read its list.

The controls on Subscription Edition

CONTROL	WHERE IT IS SET	HOW ITS STATE IS READ	OWNER AFTER THE PROJECT
Who creates site collections	Self-service site creation, per web application; the Create Subsites right	Central Administration, per web application	Farm owner
Quotas and locks	Quota templates; Site Collection Quotas and Locks	That page, per site collection	Farm owner, with site collection administrators
Unused sites	Site Use Confirmation and Deletion	That page, per web application	Farm owner
Permission levels and policies	Site permission levels; each web application's User Policy and Permission Policy	Central Administration, Manage web applications	Farm owner; site owners for their sites
Auditing and information management policies	Site collection audit settings; Site Collection Policies	Each site collection's settings and audit log reports	Site collection administrators, for the records owner
Service accounts and certificates	Managed accounts and automatic password change; certificate notification contacts	`Get-SPManagedAccount` ; `Get-SPCertificateNotificationContact`	Farm owner, with the directory team
Updates	The calendar of Chapter 42	`Get-SPProduct -Local` on every server	Farm owner

Sources: self-service site creation, quota templates, unused site collections, permission policies, information management policy, audit settings, Get-SPManagedAccount and Get-SPCertificateNotificationContact, all checked on 7 November 2026.

The defaults are tight; changes are local. By default only farm administrators create site collections, and anyone with Full Control or Manage Hierarchy on a site can create subsites (self-service site creation, above). A changed quota template does not reach site collections already using it, and versions and recycle bins count against the limit (quota templates, above). A user policy applies a level such as Full Control or Deny All across every site collection in a web application, and site permissions decide only what it neither grants nor denies (permission policies, above). Site use confirmation can delete a site collection whose owner does not answer, and automatic deletion "permanently removes all the content" (unused site collections, above); we would keep it off wherever a site is held for an obligation, as Chapter 26 decides.

Audit and policy live in each site collection. Information management policies carry retention and auditing for content types, lists and libraries (information management policy, above). Microsoft's audit page names SharePoint Server 2013 to 2019 but not Subscription Edition, and says that with trimming on, audit data is kept for zero days by default and deleted at the end of the month (audit settings, above). We do not know whether Subscription Edition differs, so we would have the records owner read each site collection's settings before relying on its log.

Passwords need two teams. SharePoint services "do not support" managed or group managed service accounts (service accounts, checked on 7 November 2026), so each password lives in SharePoint's managed accounts or in somebody's diary. If the directory and the farm disagree on one, "services in the SharePoint farm won't start", and change notices go by email to farm administrators (automatic password change, above). The directory team and the farm owner agree who changes each password, and the Farm Administrators group holds people who read that mail.

Review dates: the platform sets some, you set the rest

Review dates sort by basis, as Chapter 6's rules do. Audit (Standard) keeps records for 180 days; Audit (Premium) keeps SharePoint records for a year for users with the licences Microsoft lists, and a retention policy reaches ten years with an add-on (audit retention, above), so a review needing the log falls inside its window. Neither the dashboard nor `Get-UnifiedAuditLogRetentionPolicy` shows the default policy (same source), so the record states it from the licences. Auditing is off by default for some business plans, and its state is read in Exchange Online PowerShell, because the same cmdlet in Security & Compliance PowerShell always returns `False` (turning audit on, above). A build is supported for a year (Chapter 42). Everything else is your convention: we would review roles, policies and creation settings quarterly and sharing monthly, with the reason beside each date.

Each review reads every control the documented way and reports one of three states: as recorded, changed, or not read. A change goes to its owner; an unread control is reported unread, as Chapter 6 asks of every unknown. The review never adds controls into a figure: three changes are three findings, not a score.

The hand-over record

Each control gets one row: the setting and its value on the day of hand-over, the reading and who can run it, the owner and a deputy by name, the review date and its basis, and who grants exceptions. The owner takes the first reading the documented way, not from the project's notes, before signing. **A control is handed over when its owner can read its state without asking the person who set it.** The record is kept beside the verification record Chapter 9 archives.

Out of scope

Hypercare is Chapter 37, decommissioning the farm Chapter 38, measuring success Chapter 40 and lessons learned Chapter 41. Retention schedules and label taxonomies belong to their owners. Conditional access, device and network controls, Teams and OneDrive governance, adoption and licensing are not covered.

Before you continue

- [ ] The project's accounts, apps and policies left every role, group and site, and the assignments were read again
- [ ] Every password the project knew was reset on the day it closed
- [ ] Every control has a named owner and deputy who stay after the project
- [ ] Each owner took the first reading the documented way, sharing and labels one site at a time
- [ ] Groups and sites kept for an obligation are outside expiration, inactivity and deletion policies, or their records owner agreed
- [ ] Every review date names its basis: a documented window, or your convention with its reason
- [ ] Each review reports every control as recorded, changed or not read, never as one figure
- [ ] The record was signed before the project closed and kept beside Chapter 9's verification record