ACCESS MANAGEMENT PROCEDURE

Quarterly Access Review

Lakeside Logistics Co. · 60 staff, 9 business systems

Document ID	IAM-PR-003	**Version**	1.1
Owner	IT & Security Manager	**Effective**	February 3, 2026
Frequency	Quarterly (Jan, Apr, Jul, Oct)	**Review cycle**	Every 12 months

SAMPLE DOCUMENT. Lakeside Logistics Co. is a fictional business. This sample shows the format and depth of a Next Wave Capital Ventures documentation deliverable. Names, systems and details are illustrative.

1. Purpose

Access tends to grow over time: people change roles, contractors finish, and old accounts linger. This procedure makes sure every person's access is still needed and appropriate, removes what isn't, and keeps the evidence an auditor or customer security review will ask for. It supports common audit expectations for logical access, such as SOC 2 criteria CC6.1–CC6.3.

2. Scope

- All in-scope systems listed in the System Register: Microsoft 365, the transportation management system (TMS), accounting, payroll, the warehouse system, VPN and cloud admin consoles.
- All account types: employees, contractors, shared/service accounts and administrator accounts.
- Administrator and finance-system access is reviewed every quarter. Standard user access in lower-risk systems may be reviewed twice a year if the System Register says so.

3. Roles

Role	Responsibility
IT & Security Manager	Runs the campaign, exports access lists, tracks completion, keeps the evidence.
Reviewer (people manager)	Confirms each direct report's access: keep, change or remove. Cannot review their own access.
System Owner	Reviews shared, service and admin accounts on their system, and access with no manager.
HR	Provides the current staff list, role changes and leavers for the quarter.
Leadership sponsor	Signs off the completed review and approves any exceptions.

4. Procedure

Week 1: Prepare

#	Step	Owner	Done
1	Pull the current staff and contractor list from HR, including leavers and role changes since the last review.	IT & Security Mgr	☐
2	Export user and permission lists from every in-scope system. Save the raw exports, dated, in the evidence folder.	IT & Security Mgr	☐
3	Match each account to a person and their manager. Flag accounts with no match (orphans) and leavers who still have access.	IT & Security Mgr	☐
4	Remove leaver access immediately. Do not wait for the review to finish.	IT & Security Mgr	☐

Weeks 2–3: Review

#	Step	Owner	Done
1	Send each reviewer their team's access list with a due date (10 business days).	IT & Security Mgr	☐
2	Mark every line Keep, Change or Remove, with a short reason for anything unusual.	Reviewer	☐
3	Review shared, service and administrator accounts on each system. Confirm each has a named owner.	System Owner	☐
4	Check for conflicting access (segregation of duties), e.g., one person who can both create vendors and approve payments.	IT & Security Mgr	☐
5	Chase overdue reviews at day 7 and escalate to the leadership sponsor at day 10.	IT & Security Mgr	☐

Week 4: Fix and close

#	Step	Owner	Done
1	Make every Change and Remove decision in the system. Removals within 5 business days; admin access within 1.	IT	☐
2	Re-export permissions and confirm the changes took effect. Save the "after" export.	IT & Security Mgr	☐
3	Record any approved exceptions (access kept despite a conflict) with an owner, reason and expiry date.	Leadership sponsor	☐
4	Complete the quarterly summary (section 6) and get leadership sign-off.	IT & Security Mgr	☐

Rubber-stamping check: if a reviewer approves 100% of access with no changes two quarters in a row, the IT & Security Manager spot-checks five of their lines with them. Reviews must be real decisions, not a formality.

5. Evidence to keep (24 months)

Evidence	What it proves
Dated "before" exports from each system	What access existed when the review started
Completed reviewer worksheets (Keep / Change / Remove)	Each line was reviewed by the right person
Change tickets or logs for removals	Decisions were acted on, and when
"After" exports	The removals actually took effect
Exceptions register and signed summary	Leadership accepted remaining risk knowingly

6. Quarterly summary (example: Q1 2026)

Measure	Q4 2025	Q1 2026	Target
Accounts reviewed	412	398	100%
Reviews completed on time	84%	96%	≥ 95%
Access removed	37	14	—
Leaver accounts found still active	3	0	0
Orphan / ownerless accounts	6	1	0
Open SoD exceptions	2	1	Each with expiry

Sign-off: IT & Security Manager _____ Leadership sponsor _____ Date _____

7. Revision history

Version	Date	Change
1.0	Aug 4, 2025	First version.
1.1	Feb 3, 2026	Added segregation-of-duties check, rubber-stamping check and quarterly metrics.