CHECKLIST

Separation and Access-Termination Checklist

What this is	Same-day closeout of systems, devices, keys, records, and final pay — with the record it produces.
It assumes	A systems inventory. If you do not have one, build that first; it is also on the Open Shelf.
Change before use	The system list, and who holds administrative rights for each.

THE RECORD IS THE SPREADSHEET

The list below is what has to happen. **The record that a reviewer will ask for is the accompanying spreadsheet** — one line per system with the date, the time, and the initials of who closed it and who verified it, plus the property, pay, and handover sheet.

The figure at the foot of that sheet is the number of systems with no closure recorded. It should be zero before the file is filed.

Why same-day

A departed employee with live access to client records is a data-protection exposure with no compensating benefit, and it is one of the easiest findings for a reviewer to make: they sample your user lists against your separation dates. The fix costs nothing — a checklist run on the last day, every time, by a named owner.

The checklist

Employee: ____ **Role:** **Last day:** **Checklist owner:**

Before the last day

- Handover of open work documented: cases, deadlines, and where the files live — reviewed by the supervisor.
- Passwords for any shared or service accounts the person knew scheduled for rotation on the last day (then eliminate the shared account — see the systems inventory).
- Final pay calculated per applicable law, including accrued amounts; payroll notified of the date.

On the last day — access

- Every system account disabled, from the systems inventory list — not from memory. One line per system, initialed, timed.
- Email: account disabled; forwarding or delegate access set per policy for [30] days, then closed.
- Remote access, VPN, and multi-factor tokens revoked.
- Shared/service account passwords rotated as scheduled.

- Removed from distribution lists, group chats, on-call rotations, and any external portals (funder systems, county systems, bank access) — external portals are the ones most often missed.

On the last day — property

- Devices returned and logged against the equipment record; personal-device access to organizational data removed where applicable.
- Keys, badges, cards returned; door codes changed if the person had codes rather than a badge.
- Files and records in the person's possession returned; nothing organizational remains in personal cloud or email — the person confirms in writing.

Within one week

- Exit conversation held and documented where the person is willing.
- Personnel file completed: separation date, reason category, rehire eligibility, final pay evidence, this checklist.
- COBRA / benefits notices issued per applicable requirements.
- The role's duties reassigned by name on the accountability map — a vacant row is a finding on your own map.

Owner's confirmation: every applicable line above is complete. Signature: _____________ *Date:*

The quarterly test

Once a quarter, someone other than the checklist owner pulls the user list from two systems and checks every account against the current roster. Any live account belonging to a departed person is logged as a finding through the corrective-action protocol — because the interesting question is not the account, it is why the checklist missed it.

Published by The CARES Collaborative, a program of Knotts Family Services, Inc., for adaptation and use by charitable and community-serving organizations. No registration, no fee, no attribution required. This document is a working template, not legal, tax, or accounting advice — the requirements that apply to your organization are confirmed by your own counsel, auditor, and licensing authority. Version 1.0 · August 2026 · carescollaborative.org/open-shelf