FIRST EDITION · 23 NOVEMBER 2026

A Practical Guide to Employee Role Changes and Terminations at Banks and Credit Unions

Keep the decision, the work, and the evidence connected

A role change should give an employee the access needed for the new job without quietly carrying forward permissions from the old one. A termination should remove access, transfer ongoing responsibilities, and leave an honest record of anything still unresolved.

This guide is for bank and credit union operations managers and IT administrators. It offers a process you can use with a controlled spreadsheet, a ticketing system, or access-coordination software. Purchasing RightRole is not required.

How to use this guide

- **Set ownership and timing:** pages 2–3.
- **Run the change:** role changes on page 4; terminations on page 5.
- **Verify and close:** pages 6–7.
- **Discuss realistic examples:** pages 8–9.
- **Copy the working tools:** checklists on pages 10–11; blank change record on page 12.
- **Understand RightRole's role:** page 13.

Three kinds of guidance

Recommended practice describes a general process to consider and adapt. Most of this guide is recommended practice, not a statement about any software.

Institution policy decision identifies choices your institution must make: who can authorize changes, required timing, verification independence, exception authority, evidence handling, and retention. Have the appropriate internal owners approve those choices.

RightRole capability appears only in the concluding section. The reusable tools recommend a broader record than any claim about fields or attachments supported by RightRole.

> **Educational guidance, not an institution's approved procedure.** This is not legal or regulatory advice, a certification of controls, or a substitute for your institution's approved procedures. It prescribes no universal access deadline or retention period. All worked scenarios, people, institutions, identifiers, systems, approvals, and evidence references are fictional.

FIRST EDITION · 23 NOVEMBER 2026

1. Assign responsibility before the request arrives

Recommended practice. Name one change coordinator to follow the whole event, but assign each system action to a specific administrator. A group inbox can receive work; it does not by itself identify who will perform it. Confirm that a backup can act and has the necessary authorized privileges.

Responsibility	Accountable action	Handoff or record
HR or authorized event source	Confirm employee identity, event type, effective timing, and permitted recipients.	Authorized request reference; changes or cancellations.
Current and receiving managers	Explain old and new duties; identify continuing responsibilities and requested access.	Business need for retained, added, or removed access.
Authorized approver / system owner	Approve the permission scope within delegated authority; resolve conflicts and exceptions.	Decision, approver, timestamp, and conditions.
Change coordinator	Reconcile scope, confirm owners and backups, track timing, escalate gaps, and assemble closeout.	One record linking decisions, work, and unresolved items.
System administrator and backup	Acknowledge ownership; execute approved actions in each external system; confirm the outcome.	System/account/permission, action, actor, time, and result.
Designated verifier	Compare results with the approved target and record supporting evidence.	Verification method, result, verifier, time, and evidence reference.
Exception authority / closeout reviewer	Decide residual-risk treatment and whether closure criteria are met.	Named exception owner, next review, and final disposition.

Institution policy decision. Map these responsibilities to your organization. One person may hold several roles, but document where a separate approver or verifier is required. Do not describe a self-check as independent verification. Establish an escalation contact and alternate for unavailable owners, disputed authority, and urgent events.

Set up coverage, not just names

Maintain a controlled system list with primary owner, backup, support route, privileged-access requirements, and known dependencies. Include externally hosted services and vendor-managed accounts. Agree who can contact vendors and who can authorize emergency action outside normal hours. Test contact availability through your approved process.

For an employee who is also an administrator or manager, assign successors for systems, backup duties, managed staff, approvals, and unfinished work. Do not leave continuing responsibilities assigned to a departed or transferred employee.

FIRST EDITION · 23 NOVEMBER 2026

2. Capture an authorized request and an exact time

Recommended practice. Start one change record per employee event. Verify the request through an approved channel and match a stable employee identifier to the correct accounts; a name alone is not enough. Collect only necessary personnel information. A technical work item rarely needs the reason for an employment decision.

Minimum intake

- Employee identifier, display name, current role/location, receiving role/location if applicable, and manager or authorized contact.
- Event type, request reference, requester, authorization evidence, approver, approved permission scope, and decision timestamp.
- Effective **date, clock time, and timezone**; identify the UTC offset for that date when ambiguity is possible. Record separate action windows where systems must be sequenced.
- Affected systems, account identifiers, permissions/groups, privileged or alternate identities, remote access, physical resources, and operational handoffs.
- Coordinator, per-system work owner and backup, verifier, escalation contact, and agreed acknowledgement and completion targets.

Resolve timing before execution

Distinguish the requested effective time from a task's due time and its actual completion time. Use an unambiguous notation, such as “2026-12-07 09:00 America/New_York (UTC−05:00).” This is an illustration, not a recommended deadline. Reconfirm any timezone or daylight-saving ambiguity.

Institution policy decision. Define risk-based deadlines, after-hours coverage, permitted early preparation, emergency authority, and who can change the effective time. For urgent terminations, use the approved confidential coordination channel and escalation procedure; do not improvise a new approval route from this guide. Do not delay a policy-required protective action merely to perfect the paperwork.

If the request is incomplete or changes

Resolve uncertain identity, missing authority, or contradictory permission instructions before making discretionary changes. Escalate according to policy if the timing is urgent. Record what is unknown and who must decide; do not treat silence as approval.

When an event is changed or cancelled, authenticate the new instruction, version the approved target, notify all owners, and reconcile actions already taken. Stop superseded tasks through the approved process. Reversing a completed removal is a new authorized action, not an automatic return to the old state.

> **Keep the record distinct.** “Requested” means someone asked. “Approved” means an authorized person accepted a defined scope. Neither means the target system has changed.

FIRST EDITION · 23 NOVEMBER 2026

3. Run a role change without accumulating access

Recommended practice. Compare three things: the employee's current recorded access, available evidence of actual external access, and the approved needs of the new duties. A job-title baseline helps organize the comparison; it is not proof that every employee has exactly that access.

A. Build the system-by-system decision

For every relevant account and permission, propose **retain, add, remove, or investigate**. Include permissions unique to the employee, nested groups, delegated rights, elevated accounts, shared-resource membership, and local accounts outside central sign-in. Investigate unknowns rather than treating an empty inventory as “no access.”

Ask the receiving manager to explain the business need for retained and added access. Ask the former manager or system owner which old duties have ended. Have the authorized approver resolve conflicting permissions, separation-of-duty concerns, and any required additional review under local policy.

B. Approve overlap deliberately

Do not retain old access indefinitely “in case it is useful.” If a handover needs overlap, specify exact permissions, business reason, approving authority, start and end, compensating measures, owner, and removal/review trigger. Track the expiry as assigned follow-up work. A requested exception is not an approved exception.

C. Sequence and execute

Coordinate removal and addition order to avoid unauthorized overlap or an avoidable service interruption. Prepare changes in advance only when approved and technically safe. Assign one owner and backup for each action; ask owners to acknowledge the scope and time.

Administrators act in the external systems using approved methods. Record actual execution times and outcomes, including partial success. If a permission name or account differs from the request, stop that disputed action and obtain clarification rather than granting a convenient substitute.

D. Verify and review

Confirm required new access and removal of obsolete access against the approved target. Use the verification methods on page 6. Confirm retained access is still justified; “no change” is a decision, not a reason to skip review.

Reassign old operational responsibilities and unresolved tasks. Give the receiving manager an appropriate summary, protecting sensitive access details. Close only when the criteria on page 7 are met; keep handover exceptions and their expiry visible.

Institution policy decision. Set approval levels, conflict rules, overlap limits, verification depth, and which role changes need follow-up review. This guide does not supply a universal permission model.

FIRST EDITION · 23 NOVEMBER 2026

4. Coordinate a termination across all access paths

Recommended practice. Use the authorized event and confidentiality rules to coordinate the effective time. For an urgent event, activate the institution's approved procedure and escalation contacts. Confirm that owners have received the instruction; sending a message is not proof of action.

A. Establish scope and sequence

Reconcile the system list against available account evidence and manager input. Include central identity, local/vendor accounts, privileged identities, remote access, active sessions, authenticators, mobile devices, delegated access, and physical entry as applicable. Identify dependencies and vendor-only actions. Do not assume disabling central sign-in closes every path.

Keep employee sign-in removal separate from permitted business continuity. Mailbox access, work reassignment, file ownership, shared credentials, and service identities need approved treatment. Do not indiscriminately disable a shared/service identity or delete records that other processes depend on. Transfer ownership and rotate exposed shared credentials through authorized procedures.

B. Execute at the coordinated time

Each administrator performs the approved revocation or disablement and any applicable session/token or remote-access actions supported by the target system. Identity providers and applications can behave differently; verify the relevant paths rather than assuming one action propagates everywhere.

Track badges, keys, devices, and other operational items separately. An asset returned does not prove a software account was disabled; an account disabled does not prove a badge was recovered.

C. Verify, escalate, and transfer responsibility

Record what was actually disabled or removed, by whom and when, then verify against the authorized target. If a system is unavailable or vendor action is pending, record the exposure, use only approved containment measures, and escalate to the named authority. Keep the affected item blocked or awaiting verification; do not mark it complete to clear the queue.

Assign successors for the employee's system ownership, backup duties, managed employees, approvals, and unfinished work. Confirm the successors accept the responsibilities.

D. Preserve the right records

Apply approved preservation, records-retention, and disposal procedures before deletion. Consult the appropriate internal authority about any hold or investigation. Archiving an employee record is an administrative record action, not evidence that external access has been revoked.

Institution policy decision. Determine urgency categories, coordination sequence, notification recipients, preservation requirements, and closure authority. This guide sets no universal termination deadline and does not replace approved emergency procedures.

FIRST EDITION · 23 NOVEMBER 2026

5. Verify the outcome, not just the task status

Recommended practice. Treat these as four separate layers. A record at one layer does not automatically establish the next.

Evidence layer	What it answers	What it does not establish
Requested change	What did someone ask to change?	Valid authority or completed work.
Approved expectation	What exact access should exist after the event?	Actual account state in an external system.
Administrator confirmation	Who reports performing which work, and when?	An independent check of the external result.
Verification evidence	What source was checked against the approved target, by whom and when?	Continuous monitoring or certainty beyond the source's scope and time.

Choose evidence appropriate to the system and risk

Use an authorized administrator view, dated access export, relevant activity/configuration log, vendor confirmation, or another institution-approved source. Identify the account and exact permissions, source timestamp, collection time, verifier, result, and limitations. An old export may predate the change; a central-directory view may omit a local account.

For additions, check the intended permission without introducing extra privilege. For removals, check absence or disabled state and relevant alternate paths. Confirm session behavior where required by your procedure. Do not use the former employee's password, request MFA codes, or perform unauthorized sign-in tests. A safe validation method should not require impersonating the employee.

Compare approved target to observed result per item. Record **pass, mismatch, or unable to verify**. Route mismatches to correction work with an owner and due time. If the implementer self-checks, identify that fact. Where policy requires independent verification, a different authorized person must perform and record it.

Store references safely

Keep evidence in an approved, access-controlled repository. Record a durable reference, description, relevant timestamp, and access restrictions. Do not copy secrets, session tokens, unnecessary personnel details, or customer/member information into a change log. Redact sensitive content using an approved method.

Institution policy decision. Select evidence standards, independence requirements, secure storage, permitted recipients, and retention/disposal periods. A screenshot or export can support review, but neither independently certifies a control or guarantees compliance.

FIRST EDITION · 23 NOVEMBER 2026

6. Manage exceptions and close without hiding open work

Recommended practice. Give every line a useful status: **awaiting approval, ready, in progress, blocked, awaiting verification, or verified complete**. These are suggested process labels, not a promise about software status options. Record “not applicable” with a reason and appropriate approval, not a blank cell.

Use a named escalation path

If a work owner cannot meet the agreed target, contact the backup. If coverage, authority, or technical capability is still missing, escalate to the designated coordinator and decision-maker. State the affected account/permission, current exposure, elapsed or missed target, approved containment, requested decision, and next update time.

Separate two conditions: an **approved business exception** permits a defined departure from the normal target; an **execution failure** means the approved target has not been achieved. Do not relabel a failure as an approved exception without an authorized decision.

For either condition, record the reason, scope, owner and backup, approving authority where applicable, risk/impact, permitted interim controls, expiry or next review, and linked follow-up. Recheck at the scheduled point. Expired approval needs action or renewed authorization, not silent extension.

Closeout gate

- Reconcile every scoped system and operational item; record the final disposition, including retained access.
- Confirm authorization, actual execution, and verification evidence are linked and clearly distinguished.
- Resolve mismatches or transfer approved outstanding work to a named owner with a due/review time and escalation route.
- Confirm responsibility handoffs and any time-limited access-removal follow-up.
- Have the designated reviewer record the outcome, unresolved exposure if any, closure authority, timestamp, and next review.

Institution policy decision. Decide whether a parent change may close with linked residual work. If allowed, label it “closed with approved follow-up” and keep those items open until resolved. Otherwise keep the parent open. Do not report “all access removed” when any removal is unverified or blocked.

Make the next review easier

Store the final record in the approved repository under institutional retention and access rules. Summarize useful process issues—unlisted accounts, unavailable backups, stale permission baselines—without exposing sensitive employee details. Assign improvements separately; do not rewrite the original execution history to make it look successful.

FIRST EDITION · 23 NOVEMBER 2026

7. Worked role change: retain, add, remove

Entirely fictional scenario. Willow Example Credit Union, employee EX-104 (“Jordan Example”), and all systems, roles, records, and times below are invented. The times illustrate an approved local plan, not an industry deadline or a RightRole screen.

Jordan moves from Branch Associate to Operations Analyst. Request RC-017 asks to keep teller rights for convenience. The receiving manager requests reporting access. The fictional authorized system owner approves the revised target on 2026-12-03 at 14:00 America/New_York (UTC−05:00): retain directory access, add read-only reporting, remove teller transaction rights. No teller overlap is approved.

Effective time: 2026-12-07 09:00 America/New_York (UTC−05:00). The coordinator records acknowledgement from the work owners and backups before the event. A pre-change administrator export confirms the two existing permissions below.

System / permission	Approved decision and reason	Work owner / backup
Example Directory / standard employee	Retain; needed in the new role.	Directory administrator / identity backup.
Example Reporting / read-only	Add; analysis duties require reports, not transactions.	Reporting administrator / reporting backup.
Example Teller / transaction operator	Remove; branch transaction duties ended.	Teller administrator / teller backup.

Execution and confirmation

The approved sequence removes teller rights first. The teller administrator confirms removal at 09:00; the reporting administrator confirms read-only addition at 09:03. Directory access needs no mutation; its retained state is checked. All times use the effective-time timezone above. Each confirmation names the account, permission, actor, result, and change reference.

Separate verification

At 09:10 the designated verifier compares current administrator views with the approved target: directory standard access present; reporting read-only present without transaction rights; teller transaction operator absent. Evidence references VE-01 through VE-03 point to dated extracts in the fictional controlled evidence repository. These are evidence references, not attachments assumed to exist in RightRole.

The coordinator confirms old branch duties have a successor. At 09:20 the closeout reviewer records verified completion. The original request to retain teller rights remains in the history as **not approved**; it is not presented as work that should have been performed.

Discussion prompt: Would your institution require a different approver, sequence, verifier, or safe evidence source? Put those decisions into your procedure before using this example as a model.

FIRST EDITION · 23 NOVEMBER 2026

8. Worked termination: blocked work stays visible

Entirely fictional scenario. Harbor Example Bank, employee EX-208 (“Taylor Example”), request TM-009, and every system, time, evidence reference, and approval in this example are invented.

An authorized confidential request sets the termination for 2026-12-08 at 16:00 America/Chicago (UTC−06:00). The coordinator uses the institution's fictional approved procedure, confirms scope and authorization, and receives acknowledgements from system owners and backups. The actual local policy determines the timing and emergency authority.

Scoped work	Recorded outcome	Verification / next action
Example Identity / employee sign-in and applicable sessions	Owner confirms disablement and session action at 16:00.	Separate verifier checks administrator state and relevant session record at 16:04; reference VE-11.
Example Remote / remote-access account	Owner confirms removal at 16:02.	Verifier checks dated account view at 16:05; reference VE-12.
Example Archive Portal / local account	Vendor service unavailable; no removal confirmation.	**Blocked, not verified.** Assigned portal owner; designated backup remains available.

Escalation instead of a false completion

At 16:06 the coordinator escalates the local-account exposure to the designated security authority. Central sign-in disablement is not accepted as proof that the portal's separate local account is unusable.

At 16:10 that authority approves a portal-specific network restriction as interim containment after IT confirms it applies to the relevant path. This is a fictional institution-specific decision, not a universally available safeguard. It is not recorded as account removal.

The portal owner opens vendor case VC-31, records the failed attempt and containment reference, and owns the next update at 16:30. If no response arrives, the coordinator will escalate again to the designated authority. The record identifies the residual exposure and verifier needed after vendor restoration.

Honest closeout state

Badge return is recorded separately. Ongoing system ownership and unfinished approvals transfer to named successors. The parent termination record remains **open—external removal blocked**, under this fictional institution's closure rule. No one declares all access removed or deletes the evidence.

When the vendor later acts, the administrator must confirm the action and a verifier must check the local account before that item can close. The coordinator then seeks closeout approval and coordinates review/removal of the temporary containment under the approved procedure.

FIRST EDITION · 23 NOVEMBER 2026

9. Reusable role-change checklist

Blank working tool · Copy for each event · Recommended practice

Use with the blank change record on page 12. A checked box means its requirement was met and referenced, not merely that someone sent a request. Add system rows as needed.

Record ID: _____ **Employee identifier:** _____

Authorized request / approval reference: _____

Effective date, time, timezone and UTC offset: _____

Coordinator / backup: _____

- ☐ Verify employee/account identity, old and new duties, requester authority, and approved effective timing; resolve conflicting instructions.
- ☐ Reconcile inventory and actual-access evidence, including employee-specific, privileged, delegated, local, and remote access.
- ☐ Record retain/add/remove/investigate decisions for each system and permission. Distinguish the request from the approved target.
- ☐ Obtain approvals for scope and permission conflicts; record approver, decision, conditions, and timestamp.
- ☐ For temporary overlap, record reason, permissions, authority, owner, backup, interim controls, expiry, and assigned removal/review follow-up.
- ☐ Assign owner and backup per action; confirm acknowledgement, sequence, and per-system timing.
- ☐ Perform authorized external actions; record actual account/permission outcome, actor, timestamp/timezone, and administrator confirmation reference.
- ☐ Verify retained, added, and removed permissions against the approved target; record method, source/time, verifier, result, and evidence reference.
- ☐ Record blockers, mismatches, exceptions, and escalation; assign action, owner/backup, due/review time, and next update.
- ☐ Transfer former duties, system/backup ownership, managed staff, approvals, and unfinished work to accepted successors.
- ☐ Reconcile every item; obtain closeout approval, keep follow-up open, and schedule overlap expiry checks.

Per-system record: Copy page 12's action block for each permission or coherent action. Include retained access even when no external change is needed.

Overall status / outstanding items: _____

Closeout reviewer / decision / time: _____

Linked follow-up owner / due or review time: _____

Institution policy decision. Adapt approvals, deadlines, evidence standards, and retention before use. This checklist does not define RightRole fields or replace your approved procedure.

FIRST EDITION · 23 NOVEMBER 2026

10. Reusable termination checklist

Blank working tool · Copy for each event · Recommended practice

Use with page 12's blank change record. Explain “not applicable” entries. Requested, contained, or unverified removal is not complete.

Record ID: _____ Employee identifier: _____

Authorized request / approval reference: _____

Effective date, time, timezone and UTC offset: _____

Coordinator / backup / escalation contact: _____

- ☐ Authenticate the event and authority; confirm identity, timing, confidentiality, recipients, and revised instructions.
- ☐ For urgent events, activate approved coordination/escalation; confirm owner and backup acknowledgement.
- ☐ Reconcile central and local/vendor accounts, privileged identities, remote access, sessions/authenticators, delegated access, and physical resources.
- ☐ Approve per-system actions and sequence; address dependencies, continuity, preservation, and shared/service identity ownership.
- ☐ Assign owner and backup per action, execution window, and escalation contact.
- ☐ Perform approved external removal/disablement and applicable session/token actions; record actor, time/timezone, result, and confirmation.
- ☐ Verify each relevant access path using approved evidence; record source/time, method, verifier, result, limitations, and evidence reference.
- ☐ Track devices, badges, keys, and operational items separately from software access; record outstanding returns.
- ☐ Escalate failed or unverified actions; record residual exposure, authorized containment, owner/backup, next update, and due/review time.
- ☐ Reassign system ownership, backup duties, managed employees, approvals, and unfinished work; confirm successor acceptance.
- ☐ Apply preservation and records rules; distinguish archive from external revocation; avoid premature deletion.
- ☐ Reconcile all work and obtain closeout approval. Keep residual work visible and assigned until verified resolution.

Overall status / unresolved access paths: _____

Exception or escalation reference / next update: _____

Closeout reviewer / decision / time: _____

Linked follow-up owner / backup / due or review time: _____

Institution policy decision. Set urgency, deadlines, preservation, verification, and closure rules. No universal deadline or retention period is prescribed.

FIRST EDITION · 23 NOVEMBER 2026

11. Blank change record

Reusable template · Recommended practice · Copy the action block for every system/permission

Store the completed record and referenced evidence only in approved repositories. These recommended fields are not a claim about fields or attachment support in RightRole.

Event and authority

Field	Complete for this event
Record ID / version / event type	_____
Employee identifier / display name	_____
Current role / new role / manager	_____
Requester / authorized request reference	_____
Approved scope / approver / decision time	_____
Effective date / clock time / timezone / UTC offset	_____
Coordinator / backup / escalation contact	_____
Overall status / record location / handling rules	_____

Repeatable system / permission action block

Field	Complete for each item
System / account identifier / exact permission	_____
Observed starting access / source / as-of time	_____
Requested action / reason / request reference	_____
Approved target: retain / add / remove / other	_____
Approval reference / conditions / timestamp	_____
Work owner / backup / acknowledgement	_____
Planned execution window / timezone	_____
Status / actual action / actor / time / result	_____
Administrator confirmation reference	_____
Verifier / method / evidence source and as-of time	_____
Verification time / result / evidence reference	_____
Exception or failure / exposure / authority / containment	_____
Follow-up / owner / backup / due or review time / escalation	_____

Closeout: disposition of every item _____ reviewer / authority _____ decision and timestamp/timezone _____ unresolved work references _____ next review _____ retention/hold/disposal rule reference _____

FIRST EDITION · 23 NOVEMBER 2026

12. Where RightRole supports the process

RightRole capability · Shipped features checked on 23 November 2026

RightRole coordinates employee access work for banks and credit unions: job-title expectations, employee-specific changes, administrators, and completion records. It is **an Identifi product**.

- **Define expectations.** The Access matrix connects job titles to expected system permissions. Authorized users review an employee's current/new permission comparison and deliberate overrides when requesting access or title changes.
- **Assign follow-through.** Primary and backup administrators own system work. Optional Shared Queue makes eligible work available to assigned backups; claim, release, and reassignment controls support ownership.
- **Record human work.** Administrators perform and verify approved actions in external systems, then confirm task completion in RightRole. Completion records identify the responsible person and completion; they are administrator confirmations, not independent live scans.
- **Coordinate offboarding.** Removal tasks, reassignment, and archive blockers support separate checkpoints. Archiving does not revoke external access; restoring a record does not automatically reactivate its disabled login.
- **Track related work.** Configured operation resources can generate applicable lifecycle work, such as badge return, for selected events.
- **Support later review.** Authorized reports and access history, separate system and employee reviews, and point-in-time file-based System Access Audits support examination of expectations, decisions, and differences.

Keep the boundaries clear

People still authorize, execute, and verify external changes. RightRole's Effective Date is an informational calendar date, not a clock-time/timezone scheduler or automatic future-provisioning instruction. Coordinate exact timing through your institution's approved process.

This guide recommends approval, timing, exception, and evidence-reference fields. Do not assume RightRole stores every field or general evidence attachment. Use an approved companion record and evidence repository where needed. A point-in-time upload or recorded completion is not continuous monitoring or a compliance guarantee.

Learn more: https://rightrole.work