Carrier Portal Access Management Checklist

Know who has access to which carrier portal, why, and remove it when they leave or change roles.

WHO USES IT	Agency Owner, Manager, Admin
LINES	Not line-specific
VERSION	1.0 | Last reviewed November 19, 2026
MAINTAINED BY	AgencyPacket
ONLINE	https://agencypacket.com/resources/carrier-portal-access-management-checklist

BEFORE YOU USE THIS
Review this against your agency's current processes, carrier guidelines, and E&O requirements before you put it into practice. Insurance rules vary by state, and some requirements are set at the local level, so confirm the licensing, disclosure, filing, and recordkeeping rules that apply where you operate. This resource is general guidance, not legal, compliance, or insurance advice. See our Terms at https://agencypacket.com/terms. Many states have insurance data security and breach notification rules. Check the ones that apply to you.

Purpose

Carrier portals hold client data and let people bind or change policies. Old logins, shared passwords, and former employees with active accounts are a common weak point. This checklist makes access visible and reviewed.

When to use it

Use it when you set up access, when someone joins or leaves or changes roles, and on a regular review schedule (for example quarterly).

Process owner

The agency owner or operations manager owns the process. Each carrier's administrator approves and removes users. A second person reviews the list.

Before you begin: required information

- A list of every carrier, with portal address and the agency's administrator contact
- A list of every employee and role
- Access to each carrier's user management screen, or the carrier contact who does it
- Your agency's security policy

Procedure

User inventory

- [ ] List every employee, their role, and their start date.
- [ ] Note anyone who has left in the last year.
- [ ] Note producers, CSRs, accounting, and any contractors or interns.

Carrier inventory

- [ ] List every carrier, MGA, and wholesaler portal the agency uses.
- [ ] Note the agency's administrator for each portal and a backup.
- [ ] Note the carrier contact who handles user changes.

Roles and permissions

- [ ] For each portal, list each user and their permission level.
- [ ] Match access to the job. A CSR may not need binding authority. A producer may not need billing access.
- [ ] Note who has administrator rights, and why.
- [ ] Write down the role definitions for your agency.

Approval ownership

- [ ] Decide who approves new access: the owner, a manager, or both.
- [ ] Require approval in writing for new access and role changes.
- [ ] Keep the approval with the access record.

New employee access

- [ ] Request access in the employee's own name.
- [ ] Give access only for the carriers they will use.
- [ ] Record the date requested, approved, and granted.
- [ ] Confirm the employee has set up multi-factor authentication if the portal supports it.

Departing employee and role changes

- [ ] Remove access on the last day, or earlier for terminations.
- [ ] Ask the carrier to deactivate accounts when you cannot do it yourself.
- [ ] Remove permissions that no longer fit when someone changes roles.
- [ ] Record the date access was removed, and by whom.

Multi-factor authentication and shared credentials

- [ ] Turn on multi-factor authentication for every portal that offers it.
- [ ] Do not allow shared logins. Each person uses their own.
- [ ] If a shared login is the only option, restrict it, record who knows it, and change it when anyone leaves.
- [ ] Keep passwords in a password manager. Do not write them on notes or in spreadsheets.

Periodic access review

- [ ] At least quarterly, compare each portal's user list to your current employee list.
- [ ] Remove anyone who should not have access.
- [ ] Check for unused accounts and dormant users.

- [ ] Check administrator lists.
- [ ] Sign and date the review.

Access problems and audit documentation

- [ ] Record lockouts, delays, and requests that were denied.
- [ ] Report suspected unauthorized access to the carrier and agency owner immediately.
- [ ] Keep the inventory, approvals, and review records for audit or carrier request.

Execution checklist

- [ ] User inventory current
- [ ] Carrier inventory and administrators listed
- [ ] Permissions match roles
- [ ] Approvals recorded
- [ ] New access requested in own name
- [ ] Departing access removed
- [ ] Multi-factor authentication on
- [ ] No shared logins
- [ ] Periodic review completed and signed
- [ ] Audit records saved

Exceptions and escalation

- **Carrier does not offer individual logins.** Document the restriction and the compensating steps.
- **An employee left and still has access.** Remove it now. Review activity for unusual use.
- **Carrier takes days to remove a user.** Ask for status. Make sure the person cannot reach the portal in the meantime.
- **Someone uses another person's login.** Stop it. Set up their own account.

Completion criteria

- Every portal has a current list of authorized users.
- Each user has their own login, with permissions that fit the job.
- Departed employees have no access.
- The latest review is dated and signed.

Make it yours: agency customization

This is a starting point built for independent agencies in general. Fill in the details below so it matches how your agency actually works, then keep your version with your other procedures.

Review schedule
Quarterly or other.

Who approves access
Name or role.

Password manager we use
Name.

Carriers without individual logins
List and compensating steps.

ASSIGN IT, TRACK IT
Need to assign this process to your team? Turn it into a repeatable workflow with AgencyPacket.

General guidance only, not legal, compliance, or insurance advice. Review against your agency's processes and the state and local requirements that apply to you before use. Version 1.0, last reviewed November 19, 2026. agencypacket.com/terms

https://agencypacket.com/resources/carrier-portal-access-management-checklist