

Retire a worker-built app safely

<https://prompt-to-prototype.com/lifecycle/retire/> · as of 2026-10-22

Stage 8 of 8: retire

Retire an app in order: confirm the decision, check holds, notify users, export what you keep, revoke access, dispose of the rest, and confirm it's gone (no public URL, no open storage). Triggers are below, and its data follows your retention schedule and any legal hold. As of October 2026.

Who this is for

App owners, IT staff, and the records and privacy owners who sign off on deleting data. You get the triggers, a checklist, retention rules and a check that the app is gone. About 10 minutes.

Not legal advice

Not legal advice. This page summarizes laws as of October 2026 for a general audience. It was written with an AI legal-research persona and hasn't been reviewed by a lawyer for your situation. Ask your counsel.

When should an app be retired?

The [gate matrix](#) sets the triggers. At Team and above, retire an app when its retire-by date passes without a reasoned renewal, when nobody has used it for about 90 days ([usage check](#)), when its owner has gone and no successor has taken over ([when the builder leaves](#)), or when something replaces it or its kill criteria from [intake](#) are met.

A Sandbox app follows its own clock: quarantined on day 90 without renewal, then deleted 30 days later unless registered at a higher tier. A legal hold overrides it.

Why quarantine before you delete?

Pause access, keep the data, and wait, because someone will turn out to need it. Inactivity checks with a quarantine step are a documented pattern in platform vendors' own governance guidance¹. For Team and above, about 30 days is good practice.

What is the retirement checklist?

Work through it in order and record each step in the app record. You can also [download the retirement checklist \(CSV\)](#): step, owner and the evidence to record. *Prompt to Prototype, Retire a worker-built app safely, https://prompt-to-prototype.com/lifecycle/retire/, as of 2026-10-22. Licensed CC BY-SA 4.0.*

- ☐ **Confirm the decision.** The app owner (or IT, for an orphaned app) approves it and writes the reason.

- ☐ **Check holds and retention** before anything is deleted or exported.
- ☐ **Notify users** with the date and the replacement or workaround.
- ☐ **Export what must be kept** to the location the retention schedule names.
- ☐ **Revoke access:** user and admin accounts, sharing links, API keys, webhooks and the identity-provider registration.
- ☐ **Revoke OAuth consents, agent grants and tokens** (M3). A grant outlives the app unless someone removes it.
- ☐ **Rotate any secret the app held** that other systems also use ([secrets](#)).
- ☐ **Remove integrations and scheduled jobs** in this app and in other tools that call it, and take down its DNS records and redirects.
- ☐ **Dispose of the data** that isn't kept, by the method below. Cancel the paid plan only after the export is verified and no hold applies, and check the vendor's post-cancellation deletion period first.
- ☐ **Update the [app registry](#):** status `retired`, the date, where exported data lives, and the disposal record.
- ☐ **Archive the app record and runbook** with the retirement record below.
- ☐ **Confirm it's gone** after the quarantine ends (next sections).

Don't: delete before you check retention, holds and export

Deleting first can destroy records the business must keep, or evidence in a dispute. Keep the export until the retention schedule says otherwise.

Don't: leave storage, URLs or agent tokens live

A legacy storage system, left unprotected after newer users moved to a different system, exposed about 72,000 images in a reported 2025 case². Orphaned apps keep standing access to the services they connect to (AP19)³. Retiring a component means confirming its storage is gone.

How do you handle records retention and data disposal?

Retirement ends the app, not your duties about its records. Some rules set a minimum keeping period, and others cap how long you keep personal information. Start with your own records-retention schedule, then check each data class the app held. The [app record](#) has fields for this (`retention_period`, `disposal_method`, `log_location`).

What does the app hold, and which rule applies?

What it holds	Where the rule comes from	Watch for
Business records the app created or kept	Your retention schedule, plus tax and records rules in the US and Canada	The schedule may name the system of record, not the app

What it holds	Where the rule comes from	Watch for
Prompts, outputs, agent logs and AI-generated code history	Treat as electronically stored information. Once a dispute is reasonably anticipated, the duty to preserve attaches, and a court can sanction failing to take reasonable steps (Federal Rule of Civil Procedure 37(e)) ⁴	In May 2025 a federal court ordered an AI provider to preserve output logs, including ones users had deleted, so a provider's retention promise can be overridden. The going-forward duty ended in September 2025 ⁵ . Set your own retention on purpose: "keep forever" and "delete at once" are both risky
Personal information	PIPEDA: personal information no longer needed for its purposes should be destroyed, erased or made anonymous, and organizations need procedures for it (Schedule 1, clause 4.5.3) ⁶ . Quebec, s. 23 of the private-sector act: destroy or anonymize it once the purposes are achieved, subject to any retention period a law sets ⁷ . The GDPR sets a storage-limitation maximum (Art. 5(1)(e)), but only where it applies ⁸	Maximums only. They don't override a minimum or a hold
Health-related documentation (if you're a HIPAA covered entity or business associate)	Required HIPAA documentation is kept 6 years from creation or last effective date (45 CFR §164.316(b)(2)) ⁹	That covers required HIPAA documentation, not every medical record. State law sets the rest
Card-payment logs	PCI DSS requires audit-log history of 12 months, with 3 months immediately available (Req. 10.5.1), and minimizing retained account data through retention and disposal processes (Req. 3.2.1) ¹⁰	That's audit-log retention. It isn't a general retention period for the app's data
Evidence for audit-scope apps	The compliance owner sets it, at any tier (the audit-scope flag).	Ask before you delete change logs or evidence

Legal holds. When litigation or an investigation is reasonably anticipated, counsel may order a hold. Then nothing is deleted, whatever the Sandbox 30-day timer or a retention schedule says. Quarantine is how to retire an app while a hold applies. Confirm that your platform can suspend deletion.

Secure disposal. These laws govern how you dispose, not how long you keep. Many states, for example New York (GBL §399-h)¹¹, require records with personal information to be shredded, destroyed or made unreadable on disposal. The FTC Disposal Rule (16 CFR Part 682) works the same way for consumer-report information¹². PCI DSS 3.2.1 also covers secure deletion. For Confidential and Restricted data, remove it from the app's store, backups, exports and shared drives, and from the AI provider's copies where your contract lets you ask ([contract terms](#)). Record who did it, when and how in `disposal_method`.

How do you confirm it's really gone?

1. **Browse to the old address while signed out**, and from outside your network. It should fail or redirect.
2. **Run an external exposure scan** on the old URL, domain and storage ([what the scan must check](#)), including public storage and leftover previews.

3. **Check the identity provider and the platform:** no grants, tokens, service accounts or keys remain.
4. **Look for what still calls it:** other apps, scheduled jobs and email links.
5. **Set the registry status to** `retired` once the quarantine has ended and the checks pass.

What if you're retiring a tool or a platform?

It's the same work at a larger scale: list every app and agent on it, decide whether to move, rebuild or retire each, and export the data and logs so the audit trail survives. The exit terms you checked at approval become your plan ([approve tools](#)). For a model retirement, see [AI provider model retirements](#).

Questions to ask your counsel

1. Which records in this app does our retention schedule cover, and where must they be kept after the app is gone?
2. Is any of this data, or its logs, under a legal hold, and who tells IT when a hold starts and ends?
3. Do our retention schedule and hold process cover prompts, outputs and agent logs in AI tools, and can those tools suspend deletion?
4. Which privacy law's destruction rule applies to the personal information in this app, and does a longer minimum retention rule override it?
5. Does any sector rule (HIPAA, GLBA, SOX-related audit records, tax or payment-card rules) set a minimum for what this app held?
6. If the app is in audit scope, what does the compliance owner need kept, and for how long?
7. When our AI provider keeps copies of prompts or outputs, how do we ask for deletion, and does a hold or court order limit it?

Record the decision

Keep a short retirement record using the [decision record template](#).

Illustrative composite

Title: Retire the quarterly vendor-checklist app · **Status:** accepted · **Date:** YYYY-MM-DD · **Owner:** the procurement operations owner (a role)

Context. A Team app built by a former analyst. Its retire-by date passed with no renewal, and nobody has signed in for 100 days.

Decision. Quarantine for 30 days, export the checklist history under the retention schedule, revoke sharing and the connector token, delete the working data, then retire. Counsel confirmed no hold applies.

Alternatives considered. Keep it running (rejected: nobody patches it). Delete at once (rejected: audit might want the history).

Consequences. The registry shows `retired`, the export location and the disposal method.

Assumptions and evidence

- **A-020** (Low): we expect orphaned apps to accumulate unless retirement is part of registration; test this by comparing apps with no use in 90 days against retirements each quarter.
- **A-029** (Low): we expect a 90-day Sandbox time-box to be about right; test this by tracking how many sandbox apps are renewed rather than registered or retired.

Evidence: vendor hygiene guidance, OWASP, one reported exposure, and statutes, a court rule and a preservation order for retention; no quantified data on retiring worker-built apps. Facts on this page are as of October 2026.

Related

- [Operate and support citizen-developed apps](#): the usage check that tells you to retire.
- [When the app's builder leaves](#): the owner-leaves trigger and the handover.
- [App registry](#): where the retired status and disposal record live.
- [Approve AI tools](#): exit terms and retiring a vendor.
- [Data handling](#): the data classes the retention table uses.
- [Graduate an app to IT](#): the alternative when an app has outgrown its owner.

-
1. Microsoft Learn, "Tenant hygiene" (Power Platform Center of Excellence guidance: detect resources owned by departed employees, send inactivity notices, quarantine non-compliant apps), 2026. <https://learn.microsoft.com/en-us/power-platform/guidance/coe/after-setup-tenant-hygiene> [vendor], accessed 2026-10-21. The starter kit it describes is no longer actively maintained; the capabilities are what matter here.
 2. CyberInsider, "Tea app suffers data breach exposing 72,000 users' photos and private messages", 25 Jul 2025. <https://cyberinsider.com/tea-app-suffers-data-breach-exposing-72000-users-photos-and-private-messages/> [news], accessed 2026-10-22. The article says the breach came from an unprotected legacy storage system covering users who signed up before February 2024. It says the code was "reportedly generated using AI tools"; that claim is reported, not confirmed.
 3. OWASP Citizen Development Top 10, CD-SEC-09 "Asset Management Failures" (2022; the orphan risk persists). <https://owasp.github.io/www-project-citizen-development-top10-security-risks/content/2022/en/CD-SEC-09-Asset-Management-Failures> [primary], accessed 2026-10-21.
 4. Federal Rules of Civil Procedure, Rule 37(e), failure to preserve electronically stored information. https://www.law.cornell.edu/rules/frcp/rule_37 [primary], accessed 2026-10-21.
 5. Preservation order of 13 May 2025 (ECF 33, No. 1:23-cv-11195; ECF 551 in the MDL) and stipulation and order of 9 Oct 2025 (ECF 992, No. 25-md-3143), both S.D.N.Y., in *In re OpenAI, Inc. Copyright Infringement Litigation*. The second ended the going-forward duty to preserve output log data as of 26 Sep 2025 and kept data already segregated; Rule 37(e) duties were left unaffected. Copy hosted by a law firm: <https://blogs.duanemorris.com/classactiondefense/wp-content/uploads/sites/56/2025/10/In-re-Open-AI-Inc.-Copyright-Infringement-Litig.-10.9.25-Order-ECF-No.-992.pdf> [court], accessed 2026-10-21. The primary is on PACER; a court-hosted copy was not read.
 6. Personal Information Protection and Electronic Documents Act (Canada), Schedule 1, clause 4.5.3. <https://laws-lois.justice.gc.ca/eng/acts/P-8.6/FullText.html> [statute], accessed 2026-10-22.
 7. Act respecting the protection of personal information in the private sector (Quebec), CQLR c. P-39.1, s. 23 (as amended by Law 25): destroy the information or anonymize it for serious and legitimate purposes once the purposes are achieved, subject to any preservation period an Act provides; anonymization must meet the Regulation respecting the anonymization of personal

information (published May 2024). <https://www.legisquebec.gouv.qc.ca/en/document/cs/P-39.1> [statute], accessed 2026-10-22. LegisQuébec and CanLII blocked automated fetches, so the wording is confirmed from law-firm summaries (McCarthy Tétrault, Miller Thomson, Blakes), not the primary text; read it in a browser before relying on it.

8. Regulation (EU) 2016/679 (GDPR), Art. 5(1)(e), storage limitation. <https://eur-lex.europa.eu/eli/reg/2016/679/oj> [statute], accessed 2026-10-22. Where it applies is covered on [US and Canadian laws](#).
9. 45 CFR §164.316(b)(2)(i), time limit for HIPAA documentation. <https://www.law.cornell.edu/cfr/text/45/164.316> [regulator], accessed 2026-10-22.
10. PCI Security Standards Council, PCI DSS v4.0.1, Requirements 10.5.1 and 3.2.1. https://www.pcisecuritystandards.org/document_library/ [primary], accessed 2026-10-22. Requirement text confirmed against v4.0.1 reproductions on 2026-10-22; the PCI library needs a click-through, so the primary PDF wasn't read. Req. 3.2.1 includes secure deletion.
11. New York General Business Law §399-h, disposal of records containing personal identifying information (shred, destroy or make unreadable). <https://www.nysenate.gov/legislation/laws/GBS/399-H> [statute], accessed 2026-10-22. Other states have similar laws; the count isn't cited here.
12. FTC Disposal Rule, 16 CFR Part 682. <https://www.ecfr.gov/current/title-16/chapter-I/subchapter-F/part-682> [regulator], not re-read for this page.

Prompt to Prototype, Retire a worker-built app safely, <https://prompt-to-prototype.com/lifecycle/retire/>, as of 2026-10-22. Licensed [CC BY-SA 4.0](#).