When a Departing Executive Locks Up Your IP



Why This Matters

The InfinityQ Technology Inc. v. Patel matter from the Québec Superior Court (Sept. 12, 2025) is a stark reminder that you can end up in a high-risk standoff at precisely the moment you're trying to wrap up an employment relationship. In that case, the employer alleged a CTO refused to return entrusted IP, threatened to sell it, and leveraged unpaid compensation in the narrative. The court granted strong injunctive relief, recognizing the urgency and the seriousness of breaching confidentiality duties. Even if your company never faces something this dramatic, the risk pattern is common: senior people often hold the keys—literally and figuratively—to source code, data, models, trade secrets, credentials, vendor consoles, and customer integrations.

In Canada—especially in Québec—employees owe a duty of loyalty and confidentiality to their employer during employment, with continuing obligations for a reasonable time post-employment (Civil Code of Québec, art. 2088). That duty includes not using or disclosing confidential information and not undermining the employer's legitimate interests—even after they leave—while recognizing that post-employment "loyalty" isn't a free-standing non-compete and is interpreted narrowly in Québec jurisprudence. Still, where confidential information and misuse are in play, courts will move quickly if you can meet the injunction test.

The article below answers three practical questions HR leaders asked:

1. How do we avoid hostage-style IP scenarios when terminating an executive or manager?
2. How do HR and IT make sure sensitive information can't be ransomed—especially with remote, hybrid, and BYOD realities?
3. How do we close out an executive/manager cleanly so there's no "unpaid wages" angle that complicates everything?

Along the way, I'll flag where rules differ federally and provincially and offer concrete steps you can adopt now.

The pattern behind "hostage IP" disputes—and how HR breaks it

In the InfinityQ-type fact pattern, three things tend to be true.

First, **concentration of access**: an executive has broad, often undocumented, administrator rights to your code, repos, notebooks, cloud consoles, or encryption keys. Second, **fragmented governance**: credentials, artifacts, and IP are scattered across personal devices, home servers, or external integrations the company doesn't fully inventory. Third, **cash-flow friction**: there's a dispute about unpaid salary, variable comp, vacation, or expenses. Even when that dispute isn't legally a defence to keeping IP, it complicates tone, trust, and speed.

You don't fix this on termination day. You fix it months earlier by designing your organization so that no single person can hold your IP or operational continuity hostage.

Build a system where "return" isn't a negotiation

The most reliable prevention is architectural and procedural, not litigious. HR can drive that with IT and Legal:

- **Centralize ownership and logging** (not just access): Repositories (GitHub/GitLab), MLOps and data platforms, cloud accounts (AWS/GCP/Azure), CI/CD, password vaults, signing keys, and artifact registries should live under company-owned tenants with SSO/MFA, role-based access control, and immutable audit logs—so you always know who has what and when.
- **Use company-managed identities and devices**: MDM on laptops and phones, containerized workspaces for code/data, company-issued tokens/keys stored in an enterprise vault. Personal email or personal cloud storage must never be part of the workflow.
- **Automate joiner–mover–leaver (JML)**: Termination workflows should programmatically disable SSO, rotate keys, revoke tokens, transfer repository ownership, and reassign service accounts within minutes.
- **Make custodianship explicit**: In executive offer letters and IP/confidentiality agreements, require maintained inventories of critical systems a role administers and make periodic certifications a condition of variable comp.
- **Keep escrow-like continuity hooks**: For critical encryption keys or code signing certificates, implement dual control or secret-sharing so that no single person's cooperation is required to keep operating.

Those controls dramatically reduce the chance that "returning" information is even necessary—because the definitive version never left your custody.

What to put in the contract (and policy) so your legal footing is strong

In Québec, the duty of loyalty in **CCQ art. 2088** already obliges employees to act faithfully, not disclose confidential information, and to protect the employer's legitimate interests—with post-employment duties persisting for a reasonable time. But don't rely on 2088 alone; courts emphasize its limits and expect employers to draft proper covenants where needed.

Across Canada, tighten these building blocks:

1. **IP assignment and moral rights waivers.** Ensure the executive assigns all IP

created "in the course of" employment and waives moral rights to the fullest extent permitted by law. Reference third-party work-made-for-hire where applicable.
2. **Confidentiality that survives termination.** Define "confidential information" broadly but reasonably (trade secrets, source code, models, prompts, datasets, customer terms, roadmaps). State explicit return-and-purge obligations on demand and at termination.
3. **Return-of-property and certification.** Require immediate return of all company property (devices, credentials, archives) and written certification of deletion from personal systems and accounts.
4. **Cooperation clause.** Require reasonable post-employment cooperation (e.g., assisting with IP transfer, responding to regulator questions), with a per-diem rate pre-agreed to avoid future fights.
5. **Dispute forum and injunctive relief.** Identify governing law and venue and acknowledge the employer's right to seek injunctive relief for threatened misuse of confidential information, with the employee consenting that damages would be inadequate—useful when you're meeting the **RJR-MacDonald** interlocutory injunction test (serious issue, irreparable harm, balance of convenience). (Dentons)
6. **No set-off against wages; payroll compliance.** Clarify that disputes over expenses/claims can't justify withholding statutory wages. Most jurisdictions prohibit unauthorized deductions and impose **strict deadlines** for final pay. In BC, for example, employers must pay *all wages owing* within **48 hours** when the employer terminates employment; within **six days** if the employee resigns. Federally regulated employers have their own termination/notice/severance rules under the Canada Labour Code. Québec prescribes the timing of indemnities and notice. Get this wrong and you energize the very leverage you're trying to avoid.

Termination day: how HR and IT execute a calm, defensible offboarding

Well-run offboarding is choreography: secure the environment, close out the employment promise, and preserve evidence—all while treating the person with dignity.

Lock and transfer first, then talk. Your JML automation should (a) disable SSO/MFA; (b) rotate keys and tokens; (c) transfer ownership of repos, project spaces, calendars, service accounts, and license seats to a service principal or team mailbox; and (d) preserve mailboxes and cloud storage in legal hold. If the person is remote, MDM should retrieve or wipe company containers and disable device access pending courier return. Designing this to complete in minutes eliminates "race conditions."

Run a human conversation in parallel. Once the environment is safe, conduct the termination meeting with an HR lead and a senior leader. Keep it short, factual, and respectful. Provide the written package: termination letter, statutory entitlements, common-law notice or pay in lieu (as applicable), benefit conversion options, ROE timing, and a clear checklist for returning physical items. If you're in a province with strict final-pay deadlines (e.g., BC's 48-hour rule), tell them precisely *when and how* funds will arrive.

Offer a cooperation path, not a standoff. Even if you believe there's been a confidentiality breach, lead with a neutral "return and certification" request and a reasonable window. Provide a named contact in Legal/IT and a simple process (prepaid courier, secure upload portal). Make it easy to comply.

Preserve, don't pry. Forensically preserve company systems and devices. Resist ad-hoc poking around personal accounts or BYOD areas without counsel; over-reach creates privacy exposure. Under the federal regime and provincial privacy frameworks, you should collect only what's necessary and proportionate, store it securely, and limit access. (Federally regulated employers can find termination and severance obligations summarized by ESDC; privacy rules vary by sector and province.)

Stay Switzerland in your words. No editorializing about causes or motives. If there's potential litigation, your calm, consistent tone will matter later.

If the return doesn't happen: moving fast without overstepping

When critical material isn't returned—or there's a credible threat to disclose or sell it—time matters. Courts grant urgent injunctions where you meet the standard, particularly for confidential information and trade secrets. Your counsel will apply the **RJR-MacDonald** test: show there's a serious issue, that damages won't repair the harm (irreparable harm), and that the balance of convenience favours you. Build that record in hours, not days, with:

- Clear evidence of ownership (IP assignment, policies, logs).
- Specifics: what was taken, when, and why it matters (source code paths, commit IDs, export logs, data schemas).
- Risk framing: threatened disclosure to a buyer, imminent sale, or operational paralysis.
- Proof of your own clean hands: you paid statutory wages on time, offered a reasonable return process, and preserved communications.

Your odds improve when you can show you didn't create the crisis by, say, ignoring final-pay rules or leaving access open. (Dentons)

The wage angle: closing out pay so it isn't weaponized later

A recurring theme in "hostage IP" disputes is a parallel wage dispute. Fixable—with basic discipline.

Know (and calendar) your deadlines. In BC, final wages are due within **48 hours** if the employer terminates, six days if the employee resigns. Federally regulated employers must follow Canada Labour Code rules for individual and group terminations, including severance where applicable. In Québec, indemnities and notice have specific timing expectations. If you miss these, you can face complaints, penalties, and unnecessary leverage for the departing executive.

Don't offset against wages. In Ontario and most jurisdictions, you **cannot** deduct or withhold wages for claims, equipment, or set-offs unless expressly authorized by law or by a clear, written authorization that meets employment-standards requirements. If you think there's a real claim, pay wages on time and pursue restitution separately. It protects your position and preserves your credibility with a court.

Be crystal-clear about variable comp. Executives often argue unpaid bonus, commission, or vesting. Draft plans so they address termination mid-cycle, define whether amounts are "earned and payable," and outline when proration applies. Pay what is due under the plan documents and law; dispute the rest via the plan's dispute mechanism. Ambiguity is your enemy at termination.

Use a clean settlement, but don't make return of IP a precondition to statutory wages. You can condition *ex gratia* payments or releases on cooperation, certifications, and return of materials; do **not** condition minimum employment-standards wages/severance on anything. Courts and regulators have long memories on that point. (ESDC's federal termination page is a good refresher for federally regulated employers; provincial pages spell out deadlines and content.)

Special Québec considerations (and what they mean outside Québec)

Québec's **art. 2088 CCQ** duty of loyalty continues "for a reasonable time" post-employment and permanently where privacy or reputation is at stake. Courts have emphasized that this isn't a substitute for a well-drafted non-compete or non-solicit; its scope is narrower after employment ends. But when the conduct is about **confidential information**, courts will grant robust remedies, including injunctions, to stop misuse and force return. For employers across Canada, the lesson is the same: draft real covenants but also design your systems to avoid single-custodian risks. (Éducaloi)

Remote and hybrid realities: privacy-aware security that actually works

With remote work, you can meaningfully reduce ransom-style risk without trampling privacy:

- **Company containers on BYOD.** Use MDM to deploy a managed, encrypted work container that you can wipe without touching personal photos or apps. Make this transparent in your BYOD policy.
- **Zero-trust endpoints.** Short-lived credentials, device posture checks, and per-app VPNs limit the blast radius if a device walks away.
- **No "shadow" integrations.** Prohibit personal cloud or email forwarding; monitor for exfil patterns (e.g., mass downloads) with clear, privacy-vetted monitoring policies.
- **Least-privilege, time-bound access.** Grant admin rights only when needed; expire them automatically.
- **Evidence without oversurveillance.** Log access centrally, and retain logs under a defensible schedule; don't key-log or screen-scrape without a privacy basis.

A play-by-play you can adopt now (told as a story)

Three months out: You're planning a leadership restructure. HR, IT, and Legal convene a "continuity pre-mortem." You ask: if this executive vanished tonight, could we still build, deploy, sell, and support? The answer: not fully. Over four weeks, IT moves code into corporate repos, rotates secrets into the vault, enables SSO across tools, and implements dual control on signing keys. HR quietly updates the executive's contract addendum to reaffirm IP assignment and return-of-property certifications.

Termination week: Payroll has already modeled statutory and common-law entitlements. Because you operate in BC and Ontario, you calendar the BC **48-hour** final-pay rule and Ontario's ESA timing for ROE/records. You pre-fund off-cycle payroll so wires can land within the legal window. You also confirm federal obligations don't apply to you (not a federally regulated employer), but you use the federal guidance as a double-check on process.

T-15 minutes: IT primes the JML script. Legal prepares a short, neutral return-and-certification letter plus a secure upload link and a prepaid courier label for hardware.

T-0: The meeting is brief and humane. You hand over the package, including a schedule showing what's being paid now and what will land by wire within the statutory deadline. You outline a simple "cooperation window" with a named contact and no traps.

T+10 minutes: Access is closed, keys rotated, ownership transferred, legal holds applied. Engineering keeps shipping. No one scrambles.

If trouble starts: Counsel files promptly for injunctive relief, attaching the contract, logs, and proof you paid wages on time and offered cooperative return paths. You meet the **serious issue / irreparable harm / balance of convenience** test because your record is clean and the risk is real.

What if there's already a dispute about unpaid pay?

Handle it on its own legal track. Pay statutory wages and minimums by the deadlines (e.g., BC 48-hour rule for employer-initiated terminations). If there's a bona fide dispute about bonus, commission, LTIP, or vacation calculations, isolate it in a settlement discussion with counsel. Do **not** try to "net" it against return of IP or equipment; most jurisdictions won't allow set-off against wages without proper authorization, and you'll undermine your position if you end up before a judge. (Ontario's ESA policy manual on Payment of Wages is a good illustration of the constraints.) (Ontario)

For federally regulated employers: extra notes

If you're under the **Canada Labour Code** (banks, telecoms, air/rail, interprovincial transport), your termination regime differs in notice, severance, and group-termination rules. ESDC's termination pages summarize notice/severance and special procedures for large reductions. Align your offboarding with those timelines and forms; don't let a Code-specific timing miss become leverage in a parallel IP dispute. (Government of Canada)

When to call external help

Bring employment counsel in **before** you press "end access" on a contentious executive. They'll vet the termination letter, confirm statutory/common-law entitlements by jurisdiction, and help script communications. If you suspect data misuse, add IP/technology counsel right away. Their first hour will usually pay for itself in preserved remedies and fewer missteps.

The bottom line for HR

You can't litigate your way out of an avoidable hostage scenario. Design it out. Build your employment contracts, policies, and IT architecture so that no single person can hold your IP or operations. Pay what the law requires on time—especially final pay—so wage disputes don't contaminate your position. And if you must go to court, arrive with clean hands, a tight record, and a credible harm story that satisfies the injunction test.

If you do the quiet, unglamorous work now—centralizing control, automating offboarding, tightening contracts, and treating people fairly on the way out—you'll

rarely need to rely on a judge to save your IP later. And if you ever do, you'll be ready.

Quick reference to cited rules and principles (for your files)

- **BC final-pay deadline:** all wages owing within 48 hours if employer terminates; six days if employee resigns. (Government of British Columbia)
- **Federal termination/severance overview:** Canada Labour Code guidance from ESDC. (Government of Canada)
- **Québec duty of loyalty / confidentiality (CCQ art. 2088):** scope and limits; post-employment "reasonable time." (Éducaloi)
- **Ontario wage deductions / payment rules:** ESA Part V (Payment of Wages) policy manual. (Ontario)
- **Injunction test (RJR-MacDonald):** serious issue, irreparable harm, balance of convenience. (Dentons)

> **Employment Contract:** Unpaid Executive Can't Hold Company's Intellectual Property Hostage
>
> Insisting that he was owed nearly $80,000 in unpaid salary and vacation, a Chief Technology Officer refused to return the intellectual property his company entrusted to him. In addition to violating his contractual duty to keep the information confidential, the company claimed that the CTO's refusal and threats to sell the information interfered with its agreement to sell those IP assets to a Singapore-based software firm. The Québec court agreed that the CTO committed a serious breach of his confidentiality obligations which posed a significant and urgent threat to the company and issued an order requiring him to return the information and refrain from using, disclosing, communicating, or seeking to sell it to anybody else [*Infinityq Technology Inc. c. Patel*, 2025 QCCS 3392 (CanLII), September 12, 2025].