

# Protecting Corporate Information: Employee Leaks and Just Cause Termination in Canada



In today's digital era, where confidential company information can be shared at the click of a button, employee leaks have become a growing concern for HR managers. Whether it's a deliberate act of sabotage, an unintentional breach, or an ex-employee revealing sensitive details, leaks can damage an organization's reputation, compromise client trust, and lead to financial losses.

The question many HR professionals ask is: **When does an employee leak justify termination for cause?** The answer is complex, as Canadian employment law sets a high bar for just cause termination. In this article, we explore how companies can prevent leaks, handle them when they occur, and ensure compliance with employment law.

## **What Constitutes Just Cause for Termination in Employee Leak Cases?**

In Canada, termination for cause is considered the capital punishment of employment law. Courts have made it clear that an employer must demonstrate that an employee's actions were so serious that continued employment is no longer possible. This applies to employee leaks as well.

For a termination to qualify as **just cause**, the leak must meet specific criteria:

- The information disclosed was **confidential, proprietary, or privileged**.
- The disclosure caused, or had the potential to cause, **material harm** to the employer.
- The employee's actions were **intentional or reckless**.
- There were clear **policies and agreements** in place that the employee knowingly violated.

The Supreme Court of Canada has upheld that just cause termination must be proportional to the offense. If an employee unknowingly shared non-sensitive information without malicious intent, it would likely not meet the just cause standard.

## **Real-World Case Studies: When Employers Won and Lost**

**Case Where the Employer Won: RBC Dominion Securities Inc. v. Merrill Lynch Canada Inc. (2008)**

In this case, RBC sued Merrill Lynch after multiple employees left RBC and took confidential client information with them. The court ruled in favor of RBC, highlighting that the departing employees had breached their fiduciary duty and misused confidential information. Merrill Lynch was held liable for damages.

### **Case Where the Employer Lost: Shakur v. Mitchell Plastics (2017)**

An employee was terminated for cause after allegedly leaking company information. However, the court ruled in favour of the employee because:

- The employer **failed to prove** that the leaked information was confidential.
- There was no **clear employment contract or policy** that prohibited such disclosures.
- The employer **did not issue prior warnings** or use progressive discipline.

This case serves as a cautionary tale—without well-defined policies and documentation, termination for cause is difficult to defend.

### **Preventing Leaks: The Role of Employment Contracts and Policies**

To minimize the risk of leaks, HR managers must take proactive steps when drafting employment contracts and policies. **A strong confidentiality clause is non-negotiable.**

A comprehensive employment contract should include:

- **A Confidentiality Agreement:** Explicitly stating what constitutes confidential information and the consequences of disclosure.
- **Non-Disclosure Provisions:** Detailing the obligation to protect company information both during and after employment.
- **Non-Compete and Non-Solicitation Clauses:** Preventing employees from sharing sensitive information with competitors or poaching clients.
- **Data Security Policies:** Requiring adherence to cybersecurity best practices, including password protection and restricted access to sensitive data.

Employers should also conduct regular training on **data security policies** to reinforce their importance.

### **Handling Employee Departures to Prevent Leaks**

An employee's departure presents a **heightened risk** of information leaks, particularly if they are leaving for a competitor. HR managers should take specific precautions to mitigate this risk:

- Conduct **exit interviews** to remind departing employees of their confidentiality obligations.
- Restrict or disable **access to company systems** before the final workday.
- Monitor for any **suspicious data transfers or email activity** leading up to the employee's departure.
- Request a signed confirmation that all company documents, files, and access credentials have been returned.

### **Ex-Employees: Can They Still be Held Accountable?**

Yes, ex-employees can be held liable for leaks **if they violate post-employment obligations**. Courts have ruled that confidentiality agreements remain enforceable even after employment ends. Employers can take legal action if an ex-employee:

- Discloses **trade secrets** or sensitive company information.
- Violates **non-compete or non-solicitation clauses**.
- Breaches **fiduciary duties** (applicable to executives and key personnel).

That said, **enforcement varies by jurisdiction**. Some provinces, like Ontario and British Columbia, uphold non-compete clauses only in limited cases, while Québec generally disallows them unless they are narrowly defined in scope and duration.

Legal Aspect	Ontario	British Columbia	Québec	Alberta
Enforceability of Non-Compete Clauses	Restricted, must be reasonable.	Allowed in limited cases.	Generally disallowed unless very specific.	Case-by-case basis, must protect legitimate business interests.
Employee Obligation Post-Employment	Confidentiality obligations continue.	Confidentiality obligations continue.	Confidentiality obligations continue.	Confidentiality obligations continue.
Just Cause Termination Standard	High bar for proving misconduct.	High bar for proving misconduct.	High bar for proving misconduct.	High bar for proving misconduct.

### Compliance Pitfalls: What HR Managers Must Avoid

Failure to properly address employee leaks can lead to significant legal and financial consequences. HR managers should avoid these common mistakes:

- **Assuming verbal agreements are enforceable:** Courts rely on written contracts and policies. Always document confidentiality expectations.
- **Failing to investigate before terminating for cause:** Employers must conduct due diligence and gather clear evidence before making a termination decision.
- **Over-relying on non-compete clauses:** Many provinces limit their enforceability, so employers should instead strengthen confidentiality agreements.
- **Neglecting to conduct risk assessments on departing employees:** Some employees pose a greater risk than others, particularly those with access to sensitive data.

### Conclusion

Employee leaks pose a serious threat to businesses, but employers must navigate them carefully within the bounds of employment law. **Termination for cause requires clear policies, strong documentation, and proportional responses.** By implementing well-drafted employment contracts, maintaining robust security policies, and taking proactive steps during employee departures, HR managers can protect their organizations from harmful leaks.

Ultimately, preventing leaks is about fostering a culture of accountability and trust. When employees understand the importance of confidentiality—and the potential consequences of violating it—businesses stand a far better chance of protecting their most valuable information.