Insights, News & Events

6 STEPS TECH EMPLOYERS CAN TAKE TO STRENGTHEN TRADE SECRET PROTECTIONS IN 2026

Insights
Jan 7, 2026

As competition for talent and innovation intensifies in the tech sector, employers face heightened risks of trade secret theft and data misappropriation. Recent disputes between established tech companies and spin-off startups underscore the importance of robust trade secret protection strategies. Courts continue to require that companies demonstrate they have taken *reasonable measures* to protect their proprietary information before granting relief under the Defend Trade Secrets Act (DTSA) or state Uniform Trade Secrets Acts. In this environment, tech employers must be proactive in protecting their trade secrets to reduce litigation risk and preserve their competitive edge. What six steps can tech employers take to protect their trade secrets?

1. Identify and Classify Trade Secrets

The first step is to identify and classify trade secrets through a comprehensive audit of your company's intellectual property. This includes cataloging confidential assets such as algorithms, source code, product roadmaps, pricing strategies, and customer data. Once identified, you should clearly label and tier these materials based on their sensitivity and potential impact if exposed. Explicitly mark documents as "Confidential" or "Trade Secret" and define levels of access.

2. Tighten Contracts and Internal Policies

Strong contracts and internal policies remain the foundation of trade secret protection. You should require non-disclosure agreements (NDAs) or employees, contractors,

Related People

Raeann Burgo
Partner
412.822.6630

Brett P. Owens
Partner
813.769.7512

vendors, and investors before sharing sensitive data. Where legally permissible, you should include reasonable non-solicitation, non-compete, and confidentiality clauses. You should incorporate confidentiality duties into employee handbooks and codes of conduct, and require exit certifications at offboarding to confirm the return of proprietary materials and the continuation of post-employment confidentiality obligations.

3. Control Access and Monitor Information Flow

Controlling access and monitoring information flow are also critical. You should implement both digital and physical safeguards, such as restricting access to sensitive information based on job function, using role-based controls, and securing data with multi-factor authentication, VPNs, and encrypted servers. Access should be on a "need to know" basis. Data loss prevention (DLP) tools can help detect large downloads, external device use, or unusual emailing of code or data.

4. Foster a Culture of Confidentiality

Even the best technical controls fail without employee buy-in. A culture of confidentiality is essential for effective trade secret protection. You should provide regular training to ensure employees understand what constitutes a trade secret and how to protect it. Leadership should model discretion and emphasize that confidentiality protects both the company and its employees. You should make confidential reporting channels available for employees to report suspected data misuse.

5. Plan for Departures and Potential Litigation

Employee exits are a common point of exposure for trade secrets. When employees leave for competitors, they take knowledge with them. You should immediately terminate access to accounts and facilities upon notice of departure. For high-risk exits, conduct forensic reviews of devices and network logs for evidence of data transfer. Maintaining audit trails and preserving evidence can support cease-and-desist actions or civil claims if necessary.

6. Ensure Legal Compliance and Readiness

Finally, legal compliance and readiness are essential. You must ensure your practices meet the "reasonable measures"

Service Focus

Employee Defection and Trade Secrets

Industry Focus

Tech

standard under the DTSA and state trade secret laws. Even small start-up companies with limited resources are expected to implement basic, good-faith measures. For tech employers, this requirement is especially salient because your core assets (such as source code, algorithms, AI models, training data, and proprietary business processes) are often digital, easily copied, and may be widely accessible within a small, collaborative team. In addition, NDAs and confidentiality agreements should include whistleblower immunity language as required by federal law to preserve the right to seek exemplary damages and attorneys' fees.

Conclusion

For support in selecting the most appropriate strategy for your business, please contact your Fisher Phillips attorney, the authors of this Insight, or any member of our Technology Industry Team. Make sure you are subscribed to Fisher Phillips' Insight System to receive the most up-to-date information directly to your inbox.