# Protecting Confidential Information in the Supply Chain Checklist

by A. Louis Dorny, Gordon & Rees Scully Mansukhani LLP, with Practical Law Commercial Transactions

Maintained • USA (National/Federal)

*A Checklist providing key steps that parties to supply chain agreements can take to avoid common confidentiality security breaches in the supply chain. Parties in supply chain relationships, including those involving strategic alliance partners, vendors, distributors, and resellers, can use this Checklist to help implement protective procedures, perform supply chain due diligence, ensure strong contractual protections are in place, institute appropriate operational and security measures, and take appropriate action after the business relationship ends.*



When companies engage in supply chain relationships, they share highly sensitive and valuable trade secrets and other confidential information with:

- Foreign subsidiaries.
- Strategic alliance partners.
- Third-party vendors.
- Distributors, resellers, and other supply chain counterparties.

Examples of highly sensitive and valuable confidential information include:

  

- New products.
- Marketing plans.
- Customer lists.
- Manufacturing processes.
- Acquisition or divestiture prospects.
- Software source code, binaries, libraries, and framework.

Theft, misappropriation, and unauthorized disclosure of confidential information are increasingly common, can cause companies significant harm (like crippling financial losses and liquidation) and are caused by:

- Internal threats, such as those posed by negligent or rogue employees.
- External threats, such as those posed by:
  - data thieves unrelated to the company; and
  - the company's supply chain relationships.

This Checklist:

- Provides key steps parties to supply chain agreements can take to avoid common confidentiality security breaches in the supply chain.
- Covers only selected common supply chain vulnerabilities and is not an exhaustive list of issues.

## Implement Protective Procedures

Cultivate an internal compliance culture by establishing a program to protect confidential information, including trade secrets, with policies and procedures that:

- Detail confidentiality expectations and requirements of vendors, suppliers, and partners through a code of conduct, or a supplier code of ethics, which broadly lays the groundwork for the organization's relationship with its partners, including use of confidential information (see Practice Note, Developing a Legal Compliance Program).
- Assign compliance responsibility to high-profile internal leaders. For example, appoint a chief security officer or general counsel to lead a team to:

  

    - identify and document specific classes of materials subject to confidentiality;
    - identify and document confidential information constituting protectable trade secrets under the laws of the appropriate jurisdiction;
    - implement appropriate physical barriers to restrict access;
    - implement appropriate technical barriers with cost-effective information technology security systems (proper use of passwords, encryption, and logging features);
    - use and enforce non-disclosure agreements with employees; and
    - increase company-level awareness of the internal and external threat environment.

- Clearly identify and communicate to employees the types of **intellectual property** (IP) that the company considers confidential.
- Strictly limit confidential material access to those employees and suppliers who have a need to know.
- Segment manufacturing processes across multiple suppliers to ensure the company's intellectual property is not concentrated in one place and therefore more vulnerable to theft.

## Conduct Appropriate Supply Chain Due Diligence

- To identify and evaluate counterparty risk, obtain a prospective partner's essential documents, including those regarding the entity's:
    - capability and capacity (for example, consider space, facility, adequacy and maturity of equipment, qualified resources, after-sales service, and manufacturing flexibility);
    - financial health, for example, review ownership disclosures, quick ratio, debt, equity, distribution of top five customers, cash flow, and ratings (for information on basic financial reporting concepts like quick ratio, see Practice Note, Financial Reporting in the US: Basic Concepts);
    - references (for example, measure customer and industry feedback and review compliance track record);
    - labor practices (for example, consider the entity's health, safety, compliance, security and hazard-related policies, procedures, and incidents);
    - structure (for example, consider the entity's use of subcontractors, agents, customs brokers, and transportation companies);

  

    - competing customers; and
    - licenses, permits, insurance, letters of credit, and bonds.

- Identify those suppliers, distributors, and other supply chain counterparties that have an actual or suspected history of intellectual property rights violations, trade complaints, or export control issues.
- Consider that it may be difficult to enforce legal rights against a supplier in a third-world country that has poor infrastructure, political instability, or limited regulation.
- Verify that the company's suppliers, distributors, or other supply chain counterparties have implemented nondisclosure agreements with their employees and consultants.
- Where possible, establish long-term relationships with suppliers instead of short-term or one-off contracts.

## Ensure Strong Contractual Protections

- When selecting the agreement's governing laws, consider how the laws could impact the company's ability to establish effective trade secret protection strategies. For example, consider:
    - the categories of information that the law deems worthy of confidentiality protection;
    - whether and how easily a party can seek injunctive relief to enforce its trade secret rights;
    - the foreign judicial system's effectiveness (note that the Office of the US Trade Representative publishes annual reports known as Special 301 Reports that identify intellectual property (IP) enforcement concerns for US IP owners by country, including ineffective judicial systems (for the 2020 report, see 2020 Special 301 Report)); and
    - whether to include a private arbitration clause to avoid having to litigate in an ineffective judicial system (see Practice Note, Drafting International Arbitration Agreements: An Overview).
- Review the company's supply chain terms and conditions to ensure favorable terms necessary to safeguard the company's intellectual property, for example:
    - clear language identifying the confidential material;
    - prohibitions on wrongful disclosure;
    - auditing rights procedures (see Standard Clauses, General Contract Clauses: Audit Rights);

  

    - a further assurances provision (see Standard Clause, General Contract Clauses: Further Assurances);
    - a liquidated damages or penalty term that is tied to misuse of confidential material and other intellectual property (see Standard Clause, General Contract Clauses: Liquidated Damages);
    - a requirement that the counterparty return confidential material on contract expiration or termination; and
    - an arbitration provision where beneficial, for example in a jurisdiction with weak trade secret misappropriation laws.

- Control subcontractor liability by:
    - limiting the supplier's ability to subcontract (see Standard Clauses, General Contract Clauses: Subcontracting); or
    - retaining the right to inspect or refuse the supplier's subcontractors.

- Vet the supply agreement with local counsel on critical enforceability and local compliance measures.

For more information about the structure and form of confidentiality agreements, see Confidentiality and Nondisclosure Agreements Checklist. For sample confidentiality provisions, see Standard Clauses, General Contract Clauses: Confidentiality (Short Form) and General Contract Clauses: Confidentiality (Long Form).

## Take Appropriate Operational and Security Measures

- Budget for and regularly exercise audit and inspection rights.
- Periodically request data breach information.
- Evaluate risk mitigation through available insurance instruments.

## Take Appropriate Action After the Business Relationship Ends

- Remind departing employees of their nondisclosure agreement obligations.
- Ensure departing employees timely return company materials.
- Strictly and timely enforce electronic access rights.

  

- Where appropriate, advise a competitor who has hired an ex-employee of the ongoing duty protect the company's trade secrets.

For a Checklist of legal issues to consider when an employment relationship ends through an employee resignation or involuntary termination, see Departing Employee Checklist.

  