



## Purpose

L&L Products is committed to protecting the confidentiality, integrity, and availability of its information, information systems, intellectual property, and business operations. Information security is essential to maintaining the trust of our employees, customers, suppliers, shareholders, and business partners. It is also necessary to support business continuity, regulatory compliance, customer obligations, and the long-term resilience of the company.

## Scope

This policy applies globally to all L&L Products employees, contractors, temporary personnel, consultants, third parties, information assets, systems, applications, networks, facilities, and business processes. It applies regardless of location, technology platform, ownership model, or method of access.

## Policy Statement

### Policy Principles

L&L Products shall:

- Manage information security risks using a risk-based approach aligned with business priorities and recognized industry practices.
- Protect information throughout its lifecycle according to its sensitivity, value, and criticality.
- Grant access to information and systems based on legitimate business need, least privilege, and need-to-know.
- Incorporate information security into business processes, technology initiatives, projects, and third-party relationships.
- Protect personal, confidential, customer, employee, supplier, and other sensitive information in accordance with applicable legal, regulatory, contractual, and business requirements.
- Maintain appropriate capabilities to prevent, detect, respond to, and recover from information security incidents.
- Maintain business continuity, disaster recovery, and resilience capabilities for critical operations and information assets.
- Provide regular information security awareness and training.
- Monitor, assess, and continually improve the effectiveness of the information security program.

### Responsibilities

Information security is a shared responsibility.

Executive management shall provide appropriate leadership, oversight, and resources.

Global Information Technology and Governance, Risk & Compliance shall establish and maintain the supporting information security framework, policies, standards, controls, processes, and procedures.

Business and information owners shall ensure that information and systems under their responsibility are appropriately protected.

All employees, contractors, and third parties shall comply with applicable security requirements and promptly report suspected security incidents or weaknesses.

### **Supporting Requirements**

Detailed information security requirements shall be defined and maintained through supporting policies, standards, controls, processes, and procedures.

These supporting requirements may be updated by the designated owners as business, technology, risk, legal, regulatory, and customer requirements evolve.

### **Compliance**

Compliance with this policy is mandatory.

Violations may result in corrective action, restriction or removal of access, disciplinary action up to and including termination of employment or contract, and legal action where appropriate.

### **Review**

This policy shall be reviewed at least annually and following significant changes to the organization, technology environment, business operations, legal or contractual requirements, or information security risk profile.

### **Executive Commitment**

L&L Products is committed to protecting its information, technology, intellectual property, customers, employees, and business operations.

Every individual who accesses or handles L&L Products information has a responsibility to support this commitment.

### **Questions**

Questions about this Policy can be addressed to your IT Department.



First effective date: 01 March 2024

Last review date: 01 August 2026

Next review date: 01 August 2027

A stylized blue ink signature of Christophe Carré.

**Christophe Carré**  
**CEO**