Information Security Policy

Preamble

The purpose of this Information Security Policy is to ensure the confidentiality, integrity, and availability of data and information systems under the control of L&L Products. This policy defines the principles and rules to protect against unauthorized access, disclosure, alteration, and destruction of sensitive information.

Applicability

This policy applies to all employees, contractors, and third-party entities with access to L&L Products' information systems and data contained therein. All individuals granted access (“Users”) are responsible for adhering to the rules outlined in this policy and its supporting controls, processes, and procedures, and reporting any unauthorized access or potential security incidents promptly.

Information Security Objectives

- Ensure the confidentiality of sensitive information.
- Maintain the integrity of data and information systems.
- Ensure the availability of information systems and services.
- Protect against unauthorized access, disclosure, alteration, and destruction of information.
- Comply with relevant laws, regulations, and industry standards.

Scope

This policy and its supporting controls, processes and procedures apply to all information systems, networks, and data owned or operated by L&L Products worldwide. It encompasses all employees, contractors, and third-party entities who access, manage, or maintain information resources, regardless of the physical location from which the access occurs.

Information Classification

All information assets shall be classified based on their sensitivity, and appropriate security controls shall be implemented according to their classification.

- C1-Information: Information that is intended for and available to the general public.
- C2-Information: Information that is not meant to be openly accessible to the public but does not cause negative impact on the organization if it were to become public or altered.
- C3-Information: Information that can cause minor harm to the organization if lost, altered, or disclosed.
- C4-Information: Information that can cause significant harm to the organization if lost, altered, or disclosed.

Access Controls

All Users must use a unique ID to access L&L Products systems and applications and strong passwords complying with the defined password policy.

Whenever possible, Multi-Factor Authentication (MFA) will be used for accessing sensitive systems and data.

Access privileges will be provided based on the following principles:

- Need to know – Users or resources will be granted access to systems that are necessary to fulfill their roles and responsibilities.
- Least privilege – Users or resources will be provided with the minimum privileges strictly needed to complete their roles and responsibilities.

Requests for Users' accounts and access privileges must be formally documented and approved by the data owner.

Requests for external accounts and access privileges must be clearly notified in the request and be formally documented.

Requests for service accounts and access privileges must be formally documented and approved by the Chief Information Security Officer (CISO) or designee.

Requests for Administrator accounts and access privileges must be formally documented and approved by the CISO or designee. Annual reviews of access privileges will be conducted to ensure alignment with User's roles and responsibilities.

Termination Procedures:

Access to systems is promptly revoked upon a user's termination or when access is no longer required for job responsibilities.

Exit interviews include a review of access rights and the return of all organization's assets.

Remote Access:

Remote access to organization's systems require a secure, encrypted connection, such as virtual private networks (VPNs).

Remote access activities are subject to the same security controls as on-site access.

Data Protection and Privacy

Personal and/or sensitive information shall be handled in accordance with applicable privacy laws and regulations and protected accordingly.

Incident Response and Reporting

Access to organization's systems is logged and regularly monitored for suspicious activities.

Existing User accounts and access rights will be reviewed at least annually to detect dormant accounts and accounts with excessive privileges. Examples of accounts with excessive privileges include:

- An active account assigned to external contractors, vendors or employees that no longer work for L&L Products.
- An active account with access rights for which the User's role and responsibilities do not require access.
- System administrative rights or permissions (including permissions to change the security settings or performance settings of a system) granted to a User who is not an administrator.
- Unknown active accounts.

All security events or incidents must be reported immediately to the IT department.

Physical Security

Physical access to information systems, data centers, and other sensitive areas shall be restricted and monitored.

Equipment containing sensitive information shall be physically secured.

Security Awareness and Training

Employees shall receive regular training on information security policies, procedures, and best practices.

Security awareness campaigns shall be conducted to promote a culture of security.

Compliance and Auditing

Regular security audits and assessments shall be conducted to ensure compliance with this policy and relevant regulations.

Non-compliance shall be addressed through corrective actions and, if necessary, disciplinary measures.

Enforcement

Violations of this Information Security Policy and its supporting controls, processes and procedures may result in disciplinary action, up to and including termination of employment or legal action. Non-compliance with this policy may also result in the revocation of system access privileges.

Questions

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

Effective Date: 01/03/2024

Next Review Date: 01/03/2026

Christophe Carré

CEO