Lincotek

Information Security Policy

Information Security Management Systems UNI EN ISO/IEC 27001:2022

Annex 2

Table of Contents

1. Purpose

This policy defines Turbocoating Corp. D/B/A Lincotek Surface Solutions' commitment to protect company information and the personal data it processes, in compliance with ISO/IEC 27001 and applicable laws and regulations. The goal is to ensure the confidentiality, integrity, and availability of information while supporting business activities in a highly regulated environment.

2. Scope

This policy applies to all employees, collaborators, suppliers, and third parties interacting with the IT infrastructure and information of Turbocoating Corp. D/B/A Lincotek Surface Solutions

3. Description

- **Regulatory Compliance:** Lincotek is committed to complying with all applicable laws, regulations, and industry standards, including those related to personal data protection and information security.
- **Risk Management:** A continuous process of information security risk assessment and management will be implemented. Security measures will be proportional to the identified risks, with particular focus on protecting sensitive and business-critical data.
- **Responsibility:** Every employee, collaborator, and supplier is responsible for protecting the information they interact with.
- **Access Controls:** Information access will be limited to authorized personnel following the least privilege principle. Two-factor authentication (2FA) and other security controls will be used to protect remote and administrative access.
- **Physical and Logical Security:** Data centers and operational sites will be protected with physical security measures (e.g., access control, video surveillance) and logical safeguards.
- **Identity and Access Management:** Access rights will be managed through a centralized system with clear processes for assigning, modifying, and revoking access.
- **Operational Resilience:** Lincotek will implement solutions to ensure business continuity in case of incidents, including data backup and replication plans to minimize service disruption.
- **Training and Awareness:** Ongoing training programs will be promoted to raise employee awareness of information security best practices and associated risks.
- **Monitoring and Continuous Improvement:** A continuous monitoring system will be maintained to promptly detect and respond to security incidents. Periodic reviews of the policy and security controls will be conducted to adapt to emerging risks and regulatory changes.

4. Objectives

Turbocoating Corp. D/B/A Lincotek Surface Solutions' security policy represents the organization's commitment to clients and third parties to ensure the security of information and the physical, logical, and organizational tools used to process information within the certified activities.

The information security policy is based on the following principles:

- Ensure organizational awareness of the information being handled and evaluate its criticality to support the implementation of adequate protection levels;
- Ensure personnel and collaborators have appropriate knowledge and awareness of information security issues to foster responsibility in handling such information;
- Ensure secure access to information, preventing unauthorized or improper use;
- Ensure third parties involved in information processing are fully aware of security issues and apply adequate procedures;
- Ensure that anomalies and incidents affecting the information system and security levels are promptly identified and properly managed through efficient prevention, communication, and response systems to minimize business impact;
- Ensure that access to company premises and rooms is limited to authorized personnel only, protecting areas and assets;
- Ensure compliance with legal requirements and contractual security commitments;
- Ensure detection of anomalies, incidents, and system vulnerabilities to maintain service and information security;
- Ensure Business Continuity through procedures defined in the ISMS;
- Ensure that the organization's information risk management process is well-governed and periodically updated to align with regulatory parameters within the ISMS.

The information security policy is formalized within the ISMS, continuously updated for improvement, and shared with the organization, third parties, and clients.

5. Review and Control

The Management, assisted by the Information Security Management Representative (ISMR), is responsible for the periodic review of the policy to ensure alignment with significant organizational or technological changes affecting information protection.

Reviews will be conducted periodically or following any major organizational/technological developments.

6. Regulatory References

Refer to the document **"MAN00 – Information Security Operations Manual".**

7. Terms and Definitions

Refer to the document **"MAN00 – Information Security Operations Manual"**.

8. Responsibilities

Management is responsible for the content, issuance, implementation, and update of the information security policy, aligned with the evolving business and market context. It also determines actions to take following:

- significant business developments;
- new threats beyond those considered in the risk analysis;
- major security incidents;
- changes in legislation or regulations related to secure information processing.

The main responsibilities of the Information Security Manager include ensuring the correct implementation and maintenance of the ISMS, promoting and coordinating risk analysis activities, and managing relationships with telecommunications providers and critical service suppliers.

9. Communication, Training and User Awareness

The Security Policy is communicated to all personnel, collaborators, clients, and suppliers. The Information Security Manager promotes user awareness and proper implementation of security procedures through dedicated training and information sessions, encouraging active collaboration toward more coordinated and comprehensive information security management.

Hickory NC, September 1 2025

Plant Manager – Cristian Carlini

Turbocoating Corp. D/B/A Lincotek Surface Solutions