INFORMATION SECURITY POLICY

1. OBJECTIVE

Emergent Cold LatAm (hereinafter referred to as "Emergent Cold," "ECLA," or the "Company") is the leading temperature-controlled logistics solutions provider for the food industry in Latin America.

During its operational, commercial, financial, and administrative activities, the Company processes strategic and operational information and, in certain cases, personal data relating to employees, customers, suppliers, and other stakeholders.

The purpose of this Policy is to establish the principles, guidelines, and general measures governing the protection of information managed by Emergent Cold LatAm, ensuring its confidentiality, integrity, availability, and traceability, as well as the appropriate management of risks associated with unauthorized access, use, disclosure, or modification of information, whether processed through the Company's own systems or by third parties.

This Policy constitutes an essential component of the Company's Regional Compliance and Risk Management Framework and is integrated with corporate policies and standards relating to personal data protection, information security, business continuity, incident management, and cybersecurity. Its purpose is to promote a consistent and standardized approach across all regional operations, strengthening an organizational culture focused on protecting information assets and complying with applicable legal and regulatory requirements in each jurisdiction.

Furthermore, this Policy serves as a framework for the design, implementation, and continuous improvement of security controls, internal procedures, and technology practices aimed at safeguarding the Company's information assets throughout their lifecycle and ensuring the secure, reliable, and efficient operation of business activities in all countries where the Company operates.

2. SCOPE

These guidelines apply to:

a. All information processed by ECLA, regardless of its format (physical, digital, or hybrid), location, or the means through which it is processed, transmitted, stored, or communicated.
b. All systems, applications, networks, infrastructures, and technology services used by the Company, whether managed internally or by third parties, including cloud services and Software-as-a-Service (SaaS) solutions.
c. All directors, officers, managers, employees, contractors, consultants, temporary personnel, and third parties who, under any arrangement, access, manage, or process information belonging to Emergent Cold LatAm.
d. All service providers, vendors, contractors, and third parties that directly or indirectly process, store, access, transmit, or otherwise handle Company information.

3. REGULATORY FRAMEWORK

This Information Security Policy is issued in accordance with the legal and regulatory frameworks applicable in each country where ECLA operates and is aligned with the corporate principles governing information asset protection, risk management, and compliance across the region. Its purpose is to establish a common framework for safeguarding the confidentiality, integrity, and availability of information while ensuring consistent and standardized security practices throughout the organization.

The Company also adopts internationally recognized information security standards, frameworks, and best practices, adapting them to the operational characteristics of its facilities, systems, technologies, and business processes. These standards guide the design and implementation of technical and organizational controls, as well as incident management, monitoring, training, awareness, and continuous improvement activities.

This Policy constitutes a fundamental pillar of the Company's Corporate Compliance and Risk Management Program and is integrated with regional policies, standards, and procedures governing personal data protection, cybersecurity, IT governance, and the protection of critical information assets.

This Policy is supported, among others, by:

a. Applicable laws and regulations relating to information security, cybersecurity, and personal data protection in each jurisdiction where Emergent Cold LatAm operates, including general, sector-specific, and regulatory requirements associated with the management and protection of information assets.
b. Specific regulatory obligations applicable to the Company are based on its business activities and operations, including requirements relating to information security, operational resilience, technology services, logistics traceability, fraud prevention, physical and digital security, and any regulations issued by competent authorities in the jurisdictions where the Company conducts business.
c. Internationally recognized principles, best practices, standards, and guidelines relating to information security and cybersecurity.
d. Corporate processes, policies, procedures, and standards of Emergent Cold LatAm that form part of the regional compliance, risk management, and information protection framework, including internal requirements governing technology security, personal data protection, incident management, business continuity, and any other internal governance instruments that complement this, Policy.

4. GUIDING PRINCIPLES

Information security at Emergent Cold LatAm shall be governed, at a minimum, by the following principles:

a. Confidentiality: Information shall be accessed, used, and disclosed only by authorized individuals and solely for specific and legitimate business purposes.
b. Integrity: Information must remain accurate, complete, reliable, and protected against unauthorized alteration, modification, or destruction.
c. Availability: Information and support systems shall be available when required to support business operations, service delivery, and the exercise of rights by data subjects and other relevant stakeholders.
d. Proportionality: Security measures shall be commensurate with the nature of the information, the context of its processing, and the level of risk identified.
e. Prevention and Risk-Based Approach: Priority shall be given to the implementation of measures designed to prevent security incidents and mitigate risks before they materialize.

f. Accountability: The Company shall maintain appropriate documentation, records, and evidence demonstrating the effective implementation and operation of information security controls.
g. Security by Design and by Default: Systems, processes, technologies, and projects involving personal data or critical information shall incorporate security requirements from their design stage, initial configuration, and default settings.

5. INTERNAL SECURITY MEASURES

Emergent Cold LatAm implements internal security measures that combine organizational, technical, and physical safeguards appropriate to the nature of the information processed and the level of risk identified. At a minimum, these measures include the following areas:

a. Network and Perimeter Security Controls: Perimeter protection mechanisms and network segmentation controls designed to prevent unauthorized access, detect suspicious or anomalous activities, and limit the potential impact of security incidents.
b. Protection of Corporate and Third-Party Devices and Communications: Solutions, technologies, and procedures designed to protect corporate devices, electronic communications, email systems, and other communication channels against malware, phishing attacks, unauthorized access, and similar threats.
c. Identity and Access Management: Processes and tools for managing user identities, roles, permissions, and access rights based on the principle of least privilege. This includes strong authentication mechanisms (such as multi-factor authentication), password management standards, privileged account monitoring, and access logging for critical systems and applications.
d. Security Monitoring, Detection, and Incident Response: Continuous monitoring capabilities for relevant security events, including log collection and correlation, threat detection, risk pattern analysis, and formal response and escalation procedures for information security incidents.
e. Security Testing and Continuous Improvement: Regular execution of security assessments and testing activities, including vulnerability assessments, penetration testing where appropriate, and internal or external audits of implemented security controls. These activities shall

include the documentation of findings, corrective action plans, and follow-up processes to verify remediation.

f. Backup, Business Continuity, and Recovery: Periodic backup mechanisms for critical information, together with business continuity and disaster recovery plans designed to ensure the timely restoration of systems, applications, and critical data following incidents that affect their availability.

These measures shall be reviewed and updated periodically to reflect technological developments, risk assessment results, regulatory changes, and business requirements. They may also be supplemented by technical standards, procedures, and restricted-access supporting documentation where necessary.

6. SECUTIRY REQUIREMENTS APPLIACBLE TO THIRD-PARTY PROVIDERS

Emergent Cold LatAm shall require software vendors, technology service providers, cloud service providers, and any third party that processes, stores, transmits, or accesses Company information to maintain security standards appropriate to the level of risk and sensitivity of the information involved.
At a minimum, the following areas shall be considered:

a. Protection of Information Confidentiality and Integrity
Implementation of appropriate technical and organizational measures to protect information against unauthorized access, use, modification, disclosure, or loss, including encryption mechanisms, access controls, and safeguards aligned with industry best practices.

b. Security Controls Over Critical Infrastructure and Services
Implementation of security controls for networks, servers, applications, databases, endpoints, and technological infrastructure used to deliver services to the Company, in accordance with recognized standards and the criticality of the supported operations.

c. Business Continuity and Disaster Recovery
Maintenance of documented business continuity and disaster recovery procedures that enable the restoration of services within reasonable timeframes consistent with contractual commitments and operational requirements.

d. **Contractual Security and Data Protection Commitments**
   Inclusion of specific contractual provisions relating to information security, personal data protection, confidentiality obligations, timely incident notification, regulatory cooperation, and audit or assessment rights by **Emergent Cold LatAm**, where appropriate.

e. **Secure Integrations and System Access**
   Implementation of appropriate authentication, authorization, access control, and logging mechanisms governing system integrations, data exchanges, remote connectivity, and any access to Company systems, infrastructure, or information assets.

The selection, onboarding, contracting, and periodic assessment of technology providers shall incorporate information security and personal data protection considerations from the outset, in accordance with the principles of **Security by Design and by Default** and the Company's Third-Party Risk Management framework.

7. INFORMATION SECURITY INCIDENT MANAGEMENT

Detention, reporting, analysis, containment, notification, and remediation of information security incidents shall be governed by the Personal Data Breach Incident Management Policy, applicable local Information Security Standards, and any related procedures, without prejudice to any sector-specific, regulatory, contractual, or legal obligations that may apply.

Any employee, contractor, consultant, or third-party service provider who detects or suspects a security breach, vulnerability, or information security incident shall promptly report it through the designated reporting channels and shall refrain from deleting, altering, or destroying evidence unless its preservation would further compromise the security of systems, information assets, or affected individuals.

8. TRAINING AND AWARENESS

Emergent Cold LatAm shall promote periodic training and awareness programs on information security and personal data protection for all personnel who use Company systems or process Company information. These programs are intended to strengthen the Company's security culture across the region and

within each country where ECLA operates. Training content shall include, at a minimum:

a. Identification and prevention of common threats, including phishing, social engineering, malware, and other prevalent cybersecurity risks.
b. Best practices for the secure use of passwords, devices, digital platforms, communication channels, and technology tools.
c. Internal procedures for incident reporting and management, including the roles and responsibilities of individuals involved in the response process.
d. Confidentiality obligations and personal data protection requirements, as well as the proper handling and protection of information throughout its lifecycle.

Participation in such training and awareness activities may be mandatory depending on an individual's role, level of access to information, or applicable legal and regulatory requirements within a particular jurisdiction.

9. INTEGRATION WITH THE CORPORATE COMPLIANCE PROGRAM

This Policy forms part of **Emergent Cold LatAm's Regional Compliance and Risk Management Framework** and is integrated with the Company's policies, standards, procedures, and guidelines relating to personal data protection, cybersecurity, business continuity, incident management, and other components of its internal control framework.

Compliance with this Policy shall be considered within the Company's **risk identification, assessment, and mitigation processes**, as well as within regional and local monitoring, audit, and oversight activities. Failure to comply with the provisions of this Policy may result in corrective, contractual, disciplinary, or other measures in accordance with Company policies and applicable laws in each jurisdiction.

Any amendments or updates resulting from legal, regulatory, technological, operational, or organizational changes shall be incorporated in a timely manner. Updated versions shall be communicated to the relevant stakeholders and reflected in any complementary policies, standards, procedures, and governance documents as appropriate.

10. EFFECTIVE DATE AND REVIEW

This Policy shall become effective upon its approval by the Board of Directors of Emergent Cold LatAm and shall be reviewed at least every two years, or more

frequently whenever legal, regulatory, technological, operational, or organizational changes justify such reviews.

Any amendments or updates to this Policy shall be communicated in a timely manner to the relevant stakeholders and incorporated into the related procedures, standards, guidelines, and supporting governance documentation, as applicable.