APPROVED BY
the decision No. 6 of
the meeting No. 2 of the Board of
public limited liability company
Oro Navigacija of 28 January 2026

PUBLIC LIMITED LIABILITY COMPANY ORO NAVIGACIJA
INFORMATION AND CYBER SECURITY POLICY

1. Goal	To implement efficient information security, cyber security and privacy protection of public limited liability company Oro Navigacija by managing risks that may impact aviation safety, ensuring early detection and response to incidents, increasing the resilience of public limited liability company Oro Navigacija to cyber threats and maintaining the safe and reliable operation of the networks and information systems used. Other information security management goals are defined in the strategic business plan of public limited liability company Oro Navigacija and during the management evaluation analysis.
2. Scope	Information and Cyber Security Policy is applicable to: ▪ all information and all information assets managed by public limited liability company Oro Navigacija, regardless of the form or life cycle stage; ▪ all devices and users with access to these Company resources, both at and outside the workplace, when activities are related to the functions and decisions of public limited liability company Oro Navigacija; ▪ all users of information resources of public limited liability company Oro Navigacija, including, but not limited to members of the Board, the Audit Committee, the Chief Executive Officer of public limited liability company Oro Navigacija, employees of public limited liability company Oro Navigacija, Service Providers (Suppliers) and other persons who process information on behalf of public limited liability company Oro Navigacija, in the course of performing their work or duties.
3. Policy owner	Security Division of public limited liability company Oro Navigacija.
4. Approved by	The Board of public limited liability company Oro Navigacija.
5. Policy publication	Information and Cyber Security Policy is made public on document management system of public limited liability company Oro Navigacija and external website, accessible at www.ans.lt, both in Lithuanian and English.

CHAPTER I
TERMS, DEFINITIONS AND ABBREVIATIONS USED

6.1. Audit committee	Advisory to the Board collegial body of public limited liability company Oro Navigacija.
6.2. GDPR	General Data Protection Regulation.
6.3. The Company	Public limited liability company Oro Navigacija.
6.4. Participant of ICSMS of the Company	Any management body, structural unit of public limited liability company Oro Navigacija, employee or other person named in Chapter III of this Policy.
6.5. EU	European Union.
6.6. Chief Executive Officer	The sole managing body of public limited liability company Oro Navigacija, the chief executive of the Company, responsible for organizing the operation of the Company.

6.7. Information resources	All data, information, information systems, technologies, documents and other elements related to the creation, storage, processing or transmission of information owned or managed by public limited liability company Oro Navigacija that are necessary for the activities and achievement of the goals of public limited liability company Oro Navigacija.
6.8. ICSMS	Information and cyber security management system.
6.9. LR	Republic of Lithuania.
6.10. Service Provider (Supplier)	A natural or legal person providing goods, services or works to public limited liability company Oro Navigacija when, in the course of performing a contract (or assignment), such person and/or the employees of such person are granted access to the information, information assets, restricted access premises of the Company and/or the networks and information systems of the Company, or when the services provided are related to networks and information systems or other critical information assets.
6.11. The Policy	This information and cyber security policy.
6.12. Network and information system (hereinafter referred to as NIS)	An electronic communications network, any device or group of interconnected or related devices, one or more of which automatically processes digital data under a program, or digital data stored, managed, reproduced or transmitted by specified means for the purposes of their management, use, protection and maintenance.
6.13. The Board	Collegial management body of public limited liability company Oro Navigacija.

CHAPTER II
LEGAL BASIS

7. The policy has been prepared and the provisions are applied in accordance with the requirements of EU and Lithuanian legal acts:	
7.1. EU legislation	▪ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); ▪ Commission Implementing Regulation (EU) 2017/373 of 1 March 2017 laying down common requirements for providers of air traffic management/air navigation services and other air traffic management network functions and their oversight, repealing Regulation (EC) No 482/2008, Implementing Regulations (EU) No 1034/2011, (EU) No 1035/2011 and (EU) 2016/1377 and amending Regulation (EU) No 677/2011; ▪ Commission Implementing Regulation (EU) 2023/203 of 27 October 2022 laying down rules for the application of Regulation (EU) 2018/1139 of the European Parliament and of the Council, as regards requirements for the management of information security risks with a potential impact on aviation safety for organisations covered by Commission Regulations (EU) No 1321/2014, (EU) No 965/2012, (EU) No 1178/2011, (EU) 2015/340, Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664, and for competent authorities covered by Commission Regulations (EU) No 748/2012, (EU) No 1321/2014, (EU) No 965/2012, (EU) No 1178/2011, (EU) 2015/340 and (EU) No 139/2014, Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664 and amending Commission Regulations (EU) No 1178/2011, (EU) No

	748/2012, (EU) No 965/2012, (EU) No 139/2014, (EU) No 1321/2014, (EU) 2015/340, and Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664; ▪ Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive); ▪ Commission Delegated Regulation (EU) 2023/1768 of 14 July 2023 laying down detailed rules for the certification and declaration of air traffic management/air navigation services systems and air traffic management/air navigation services constituents; ▪ Commission Implementing Regulation (EU) 2023/1769 of 12 September 2023 laying down technical requirements and administrative procedures for the approval of organisations involved in the design or production of air traffic management/air navigation services systems and constituents and amending Implementing Regulation (EU) 2023/203; ▪ Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act).
7.2. Legal acts of the Republic of Lithuania	▪ Law on Cyber Security of the Republic of Lithuania; ▪ Description of Cyber Security Requirements, approved by the Resolution No. 818 of the Government of the Republic of Lithuania of 13 August 2018 "On the Implementation of Cybersecurity Requirements of the Republic of Lithuania"; ▪ Law on the Legal Protection of the Commercial Secrets of the Republic of Lithuania; ▪ Law on the Approval, Entry into Force and Implementation of the Labour Code of the Republic of Lithuania; ▪ Law on Public Procurement of the Republic of Lithuania; ▪ Law on Approval, Entry into Force and Implementation of the Civil Code of the Republic of Lithuania; ▪ Other legal acts of the Republic of Lithuania regulating information and cyber security, as well as personal data protection.
8. The Policy is also guided by international standards and/or good practices, including:	
8.1. Good practices	▪ Lithuanian standard LST EN ISO/IEC 27001:2023 "Information security, cyber security and privacy protection. Information security management systems. Requirements (ISO/IEC 27001:2022)"; ▪ Lithuanian standard LST EN ISO/IEC 27002:2023 "Information security, cybersecurity and privacy protection. Information security controls (ISO/IEC 27002:2022)[1]".
8.2. Relevant documents	The provisions of this Policy are detailed and implemented by approving the internal legal acts of the Company that are consistent with the strategic goals, legal requirements, international standards and good practices of the Company. The internal legal acts of the Company must not contradict this Policy.
9. If there are any inconsistencies between legal acts and the Policy, the Policy shall apply to the extent that it is not in conflict with the legal acts.	

[1] The standard is adapted from the European standard EN ISO/IEC 27002:2022 "Information security, cyber security and privacy protection – information security controls".

10. The terms used in the Policy are understood as they are defined in the legal acts indicated above.

CHAPTER III
INFORMATION SECURITY MANAGEMENT SYSTEM PARTICIPANTS AND THEIR FUNCTIONS

11. All participants of ICSMS of the Company are obliged to comply with this Policy, information and cyber security requirements established in legal acts, and pre-contractual and/or contractual liabilities.

12. ICSMS of the Company contributes and holds the respectful functions and responsibilities:

12.1. Board of the Company	▪ Approve this Policy; ▪ To determine the directions, goals, objectives and principles for ensuring the information and cyber security of the Company.
12.2. Chief Executive Officer	▪ Ensure the implementation of the Policy by managing this process, undertaking the liabilities[2] and by assigning responsibility for information and cybersecurity; ▪ Ensure that information and cybersecurity risk issues are an integral part of the strategic decisions and operational processes of the Company; ▪ Allocate the necessary resources required to ensure ICSMS and manage the identified risks, including human, financial resources, processes, tools and technology.
12.3. Cybersecurity executive	▪ Ensure that the Policy and documents regulating the implementation of information and cybersecurity are prepared and periodically updated; ▪ Organize the assessments of compliance with information and cybersecurity regulations and information security risk of the Company; ▪ Organize training for the employees of the Company on information and cybersecurity issues; ▪ Coordinate investigations of NIS cyber incidents, ensure cooperation with competent authorities and initiate actions to eliminate non-compliances; ▪ Provide NIS administrator, security officer and/or users with mandatory instructions and assignments related to the implementation of the requirements set out in the documents regulating the implementation of the Policy as well as information and cybersecurity.
12.4. Security officer	▪ Ensure that the requirements set out in the Policy and documents regulating the implementation of information and cyber security are implemented in the assigned NIS, supervise the implementation of cyber security requirements and provide instructions to NIS administrators and other responsible persons in order to identify and eliminate security gaps in a timely manner; ▪ To ensure the compliance of the Company with information and cybersecurity regulations and the implementation of information security risk assessment procedures; ▪ Organize and execute the implementation and monitoring of cybersecurity measures, prepare information about incidents, participate in their investigations and provide data to the cybersecurity officer; ▪ Coordinate the training of the employees of the Company on cybersecurity topics and ensure their awareness of threats, risks and preventive measures.
12.5. Personal data protection officer	▪ Monitor the compliance with GDPR, other EU and national data protection regulations and Policy on Personal Data Protection of the Company;

[2] The obligations of the management of the Company are stipulated in Safety, Quality, Security and Compliance Policy of public limited liability company Oro Navigacija.

	▪ Advise on personal data protection impact assessment and monitor the implementation; ▪ Respond to the inquiries of data subjects regarding their rights under the GDPR and other legal acts regulating the protection of personal data; ▪ Cooperate with State Data Protection Inspectorate or other supervisory authorities on personal data matters.
12.6. NIS owner	▪ Plan NIS activities and provide mandatory instructions to NIS administrator; ▪ Ensure proper functioning and security of NIS and promote their performance; ▪ Ensure proper management of NIS problems; ▪ Plan, execute and supervise NIS projects; ▪ Search and implement new NIS solutions to increase efficiency; ▪ Perform other functions established in the Policy and documents regulating the implementation of information and cybersecurity and other legal acts regulating cybersecurity and assigned to NIS owner.
12.7. NIS administrator	▪ Manage NIS user access rights; ▪ Maintain NIS components (computers, operating systems, databases, applications, firewalls, intrusion detection systems); ▪ Manage the configuration of NIS components; ▪ Identify NIS vulnerabilities; ▪ Identify and monitor compliance with security requirements, response to cyber incidents.
12.8. Security operations centre	▪ Constantly monitor NIS activities and cybersecurity events of the Company, process and escalate them in a timely manner; ▪ Perform actions related to cyber incident management (detection, prevention); ▪ Collect information about vulnerabilities, conduct their analysis, coordinate vulnerability management solutions with affected subjects; ▪ Analyse cyber threats and respond to them; ▪ Provide cybersecurity recommendations to Company employees.
12.9. Operation continuity management group	▪ Coordinate the preparation and updating of the business continuity plans of the Company; ▪ Assess the business continuity risks and identify critical functions of the Company; ▪ Organize testing and training of the business continuity measures of the Company.
12.10. Operation recovery group	▪ Organize the restoration of the services, data and infrastructure of the Company; ▪ Implement recovery actions according to established priorities; ▪ Coordinate technical recovery actions with the structural divisions and Service Providers (Suppliers) of the Company; ▪ Analyse the recovery process and provide recommendations for improvement.
12.11. Employees	▪ During daily activities, when performing work functions and making decisions, they must comply with information and cybersecurity requirements and ensure the safe use of information and information assets entrusted to them or known to them; ▪ Protect confidential information and refrain from disclosing it to third parties without the specified permission;

	▪ Identify, assess and monitor information and cybersecurity risks, select and apply measures to manage them, in accordance with the established requirements.
12.12. Service providers (suppliers)	▪ Comply with the information and cybersecurity requirements set out in the Policy, EU and LT legal acts and contracts; ▪ Undertake the responsibility to protect confidential information by applying appropriate security measures and not to publish or disclose it to third parties without the permission of the Company, unless established otherwise in the laws and other legal acts of the Republic of Lithuania; ▪ Ensure that their infrastructure and procedures meet the applicable information and cybersecurity requirements; ▪ Undertake responsibility for the safe use of the information assets of the Company entrusted to them; ▪ Ensure that sufficient measures will be taken to manage risks related to Sub-contractors, the work they perform and the supply chain.
13. The Company cooperates with institutions of the Republic of Lithuania and international organizations that frame and implement cybersecurity policy, participates in professional forums and initiatives, shares information about information and cybersecurity threats and good security practices, in order to strengthen overall security resilience.	

CHAPTER IV
PRINCIPLES AND LIABILITIES FOR ENSURING COMPANY INFORMATION AND CYBER SECURITY

14. In order to achieve the objectives of the Policy, the Company undertakes to comply with general legal principles, information and cybersecurity requirements, to implement and constantly improve ICSMS in accordance with the international standard ISO/IEC 27001, applying innovative, risk-proportionate organizational, human, physical and technological security control solutions.				
15. In order to ensure the protection of information resources and effective risk management, the Company undertakes to adhere to the following basic information security principles:				
Basic principles:		**15.1. MANAGEMENT: to ensure consistent, risk-based and mature information security management by strengthening the awareness and responsibility for security of ICSMS participants of the Company.**		**15.2. IDENTIFICATION: to ensure that all information resources are identified, assessed and managed based on risk to adequately protect information throughout the entire lifecycle.**
		**15.3. PROTECTION: to ensure information protection by applying risk-based and regulatory control measures.**		**15.4. DETECTION, RESPONSE, RECOVERY: to ensure timely detection of security events, effective response and incident resolution, restoring operations and mitigating potential impact on the Company.**
16. The main principles of the information and cyber security of the Company are ensured in the following areas:				
16.1. Management principle	16.1.1. Responsibilities and corresponding duties have been assigned to participants of ICSMS.			

	16.1.2. Information resources are managed in accordance with all laws and other related legal requirements applicable to the Company. 16.1.3. Security risk management activities are integrated into the risk management system of the Company. A holistic approach to risk management is applied. 16.1.4. Security risk is accepted before they are cleared for use and managed during the entire lifecycle.
16.2. Identification principle	16.2.1. All information assets of the Company are clearly identified, i.e. properly inventoried and maintained, and owners responsible for them are assigned. The value of the assets and their criticality to operations are determined. 16.2.2. Requirements for confidentiality, integrity, authenticity and availability of information resources have been established and documented. 16.2.3. Information in the Company is divided into public, non-public and non-disclosed, confidential and of special importance, and is marked accordingly using the *traffic lights* method[3]. 16.2.4. Information security classification and the protection levels are determined in proportion to the importance of the asset. 16.2.5. ICSMS is based on the identification, assessment and monitoring of risks. Risk assessments are carried out at least annually or when changes occur, in order to identify and assess the various information security risks and to determine the priorities of the necessary control measures, taking into consideration the impact on the business and the likelihood of the risk occurring. The results of the risk assessment and the related decisions are documented. 16.2.6. Risk mitigation measures are implemented based on the results of the assessments. Identified risks are reduced to a tolerable risk level by applying security measures based on the risk assessment.
16.3. Security principle	**16.3.1. Physical and environment security management:** 16.3.1.1. The company has installed appropriate physical security perimeters and access control to prevent unauthorized physical access. 16.3.1.2. Physical access to the territory of the Company, NIS, infrastructure and facilities is granted only to authorized employees of the Company. 16.3.1.3. It is prohibited to film or take photographs on the territory of the Company without permission of the responsible persons. 16.3.1.4. It is prohibited to carry/bring the following items into the territory of the Company: weapons, their accessories and ammunition or their imitations, explosive devices and explosive substances or their imitations, drugs and narcotic substances and alcoholic beverages, other dangerous items that use open flames or emit/cause sparks, except for tools or devices used for direct work for which a permit must be issued. **16.3.2. Human resource management:** 16.3.2.1. All candidates are checked before starting to work at the Company. The employees of the Company are checked periodically. Checks of candidates, employees and Service Providers (Suppliers) working for the Company are carried out in accordance with the Law on Aviation of the Republic of Lithuania and the Law on the Protection of Objects Important for Ensuring National Security of the Republic of Lithuania. 16.3.2.2. Employees of the Service Providers (Suppliers) or a third party with which the employees of the Service Provider (Supplier) are related may be required to provide authorizations to work with the information of the respectful category. 16.3.2.3. Employees of the Service Providers (Suppliers) and persons working for them must have the necessary skills and/or qualifications and provide corresponding

[3] More information on *traffic lights* method can be found on official website: https://www.first.org/tlp/.

evidence, allowing them to work with a specific information resource of the Company, when necessary or required.

16.3.3. Security training and awareness raising:

16.3.3.1. The Company takes care of cyber hygiene of the employees – all employees and Service Providers (Suppliers) who are granted access to the information or information assets of the Company must be properly trained in information and cyber security matters.

16.3.3.2. At the beginning of their employment Newly hired employees of the Company must attend and complete introductory training, which also covers information and cybersecurity topics.

16.3.3.3. All employees of the Company, as well as employees of Service Providers (Suppliers) who have access to the information or information assets of the Company, must participate in training that provides knowledge on safe operations in cyberspace regularly, and the level of security awareness is consistently raised (by participating in the Company training or by providing evidence of equivalent training).

16.3.4. Access management:

16.3.4.1. Access to the information assets of the Company is granted to users authorized by the Company only. Access is reviewed regularly.

16.3.4.2. Access to the information assets of the Company is granted at the discretion of the owner of the information assets, based on the principles of least privilege and *need to know*, only for the performance of job functions or duties.

16.3.4.3. Reliable and secure identity and access management is used to access the information assets of the Company. Each user of the systems must be uniquely identified.

16.3.4.4. The employees are allowed to access the e-mail and NIS of the Company from the devices issue by the Company only.

16.3.4.5. When granting access to the information assets of the Company to third parties, confirmation from third parties must be obtained that the access will be used in accordance with this Policy and other information and cybersecurity requirements only for the specified purpose, scope and methods, and liability for violation of the specified obligation must be envisaged.

16.3.4.6. Remote access to the information resources of the Company provided to Service Providers (Suppliers) is encrypted using virtual private network (VPN) technology and with the participation of the employees of the Company in the session. Any unauthorized remote access to the information assets of the Company is prohibited.

16.3.5. Acquisition, development and maintenance of information systems:

16.3.5.1. NIS are designed, implemented, maintained, developed and liquidated taking into consideration their criticality to the operation of the Company and the requirements for confidentiality, integrity, authenticity and availability.

16.3.5.2. NIS and the components thereof are supplied and supported by reliable Service Providers (Suppliers) only. It is be prohibited to use equipment, technologies or other related services or goods from unreliable manufacturers.

16.3.5.3. Goods (including their components and manufacturers of goods and their components), services and works offered by the Service Providers (Suppliers) must not pose a threat to national security and comply with applicable requirements of international and national sanctions. The Service Providers (Suppliers) must not have business relations with entities that pose a threat to national security[4].

[4] Resolution of the Government of the Republic of Lithuania of 29 March 2022 No. 22-4687 "On the implementation of the provisions of Paragraphs 13, 14 and 15 of Article 92, the Law on Public Procurement of the Republic of Lithuania".

	16.3.5.4. NIS are designed and configured following the secure by design principle, taking into consideration security risks and all related requirements for information security control measures. 16.3.5.5. A secure software or hardware development process must be ensured at all stages: definition of the requirements, design development, implementation, validation, release, training, and maintenance. 16.3.5.6. Any new technology introduced into the Company must be approved by the responsible employees of the Company and can only be used with their permission. It is also necessary to ensure that the technologies comply with aviation safety and security requirements. 16.3.5.7. The products must contain no hidden features that could weaken security, including malicious software, unauthorized access or functions, and other security breaches. Only trusted and supported NIS may be installed in the infrastructure of the Company. 16.3.5.8. Third party software used at NIS of the Company must be in compliance with the security requirements and must be licenced. 16.3.5.9. Vulnerability assessments are performed before NIS is introduced into the operational environment and regularly during their operation, and any vulnerabilities detected are eliminated immediately. 16.3.5.10. Penetration testing is performed periodically on NIS critical to the operation of the Company, which is coordinated by authorized employees of the Company. 16.3.5.11. It is prohibited to scan NIS of the Company arbitrarily to search for vulnerabilities or monitor data traffic. Such measures may be applied only when they are necessary for the performance of direct duties and are coordinated with the employee of the Company responsible for information and cyber security. **16.3.6. Operational security of information systems:** 16.3.6.1. Computer workstations must use tools to detect, prevent and monitor malicious software and/or activity. 16.3.6.2. Log records of all Company NIS, network devices and other devices, including operating systems, databases, applications, must be stored in centralized manner. **16.3.7. Data security:** 16.3.7.1. Data is encrypted both during storage and during transmission between different NIS used by the Company. 16.3.7.2. The employees use only Company e-mail addresses (not personal e-mail or communication platform accounts) for any correspondence containing or relating to Company data. 16.3.7.3. Communication containing confidential information, including personal data, must be executed employing a secure communication channel only using a secure e-mail and document exchange solution https://cloud.ans.lt/. 16.3.7.4. The Company supports “clean desk” and “clear screen” policy, prohibiting leaving documents, files, information media, and devices containing stored information without supervision and additional protection. 16.3.7.5. Data backup copies are generated regularly and tested safely.
16.4. Detection principle	16.4.1. Event logs must be collected and analysed in real time, whereas the detected security events must be identified and managed immediately in accordance with the incident management procedures established in the Company. 16.4.2. Relevant institutions and stakeholders are notified about both internal and external safety incidents following the established deadlines.
16.5. Response and recovery principles	16.5.1. Any events that escalate into incidents are managed in accordance with incident management procedures.

16.5.2. Incident response, business continuity and plans for recovery after disasters are developed and implemented when necessary to restore normal operation during and after security incidents as well as to minimize the impact on business continuity.
16.5.3. Analysis and review are executed after every incident to improve the response and recovery procedures.

CHAPTER V
COMPLIANCE

17. In the course of operation, the Company seeks to comply with the requirements of legal acts regulating the operation, contractual obligations, and ensures compliance with this Policy. Performance assessments, internal and external audits, management reviews, and feedback from the employees and stakeholders of the Company are conducted to assess compliance with the Policy and related legal requirements. Corrective and improvement actions are identified and implemented.

18. The Company is entitled to perform an information and cybersecurity assessment or other information and cybersecurity verification actions related to the creation, development, implementation and/or use of the information resources of the Company in order to verify compliance with legal requirements and the provisions of this Policy.

19. Any failure to comply with information and cybersecurity requirements or potential and possible deviations must be documented, including the mandatory risk assessment and agreed control measures. Exceptions to the application of the Policy and related legal provisions are approved by the Chief Executive Officer of the Company, ensuring their traceability.

CHAPTER VI
LIABILITY

20. Any violation of information or cybersecurity norms is considered an information security incident that may disrupt the continuity of the operation of the Company, cause financial losses, damage to the reputation of the Company, reduce the trust of customers and partners, and lead to legal and regulatory consequences.

21. The duty to report an information and cybersecurity threat, incident or violation of requirements fall upon the members of the Board, Audit Committee, Chief Executive Officer of the Company, all employees of the Company and Service Providers (Suppliers).
In case of noticing a malfunction, security breach, cybersecurity gap or vulnerability in NIS of the Company, it is compulsory to notify Information Technology Department of the Company immediately:

✉ E-mail **cirt@ans.lt** or

☎ Telephone **+370 706 94707**.

22. The employees of the Company and the Service Providers (Suppliers), that violate this Policy and ICSMS requirements applicable in the Company, may be subject to sanctions provided for in the laws of the Republic of Lithuania, internal legal acts of the Company, contracts, agreements or other documents of legal power.

CHAPTER VII
FINAL PROVISIONS

23. Members of the Board of the Company, Audit Committee, Chief Executive Officer, all current and newly hired employees of the Company, Service Providers (Suppliers) as well as other third parties, executing contractual liabilities, are acquainted with this Policy.

24. The Policy is reviewed periodically, but at least once a year, or in the event of significant changes in the operation and regulatory environment of the Company that affect the implementation of ICSMS, and is updated as necessary.

25. The Policy is approved and amended by the decision of the Board of the Company recorded in the minutes.

_____