

VERSION CONTROL

Document Code	PL-01 GRL
Document Description	Information Security Policy
Document Type	Policy
Edition.Revision	00.00
Created by	Information Security and Systems Manager
Creation Date	2025-03-05
Reviewed by	Director of General Services and Standardization
Review Date	2025-03-05
Approved by	Information Security Committee
Approval Date	2025-03-24
Confidentiality Level	Public
Important Notice	<p>This document and its annexes are the property of GORLAN for Public Use.</p> <p>Any total or partial reproduction, as well as the use of any information contained herein, is expressly prohibited unless expressly authorized by GORLAN, holder of the intellectual property rights.</p> <p>Unauthorized persons are not permitted to consult, read or study this information. GORLAN reserves the right to initiate any legal actions deemed necessary in the event of non-compliance.</p>

TABLE OF CONTENTS

1. INTRODUCTION	3
1.1 Purpose and Scope	3
1.2 Effective Date and Validity	3
1.3 Background	3
1.4 Publication	3
2. Policy	3
2.1 Scope	3
2.2 Information Security Objectives	3
2.3 Regulatory Compliance	3
2.4 Resource Allocation	3
3. Responsibilities	4
3.1 Roles and Responsibilities	4
3.2 Chief Information Security Officer (CISO)	4
3.3 Service Owner	4
3.4 Information Owner	4
3.5 System Owner	4
3.6 Security Committee	4
4. References	4
5. Modification Control	4

1. INTRODUCTION

1.1 Purpose and Scope

This document sets out the General Information Security Policy of the GORLAN Corporate Group, understood as the basic principles governing GORLAN's actions and organisation in the field of Information Security.

1.2 Effective Date and Validity

This Information Security Policy is effective from the Approval Date of this version and shall remain in force until replaced by a new Policy.

1.3 Background

This Policy applies to all GORLAN resources and processes, as well as to all third-party services involving use and/or access to data, resources, administration and any information system control functions.

1.4 Publication

This Security Policy is available on GORLAN's SharePoint and, in its reduced public version, on the main GORLAN website.

2. Policy

2.1 Scope

GORLAN protects the resources involved in managing information related to the normal development of its activities, complying with applicable legislation, preserving confidentiality and privacy, and ensuring availability, access, integrity, quality, traceability, authenticity and preservation.

2.2 Information Security Objectives

GORLAN defines, implements, operates and continuously improves an Information Security Management System (ISMS), aligned with business needs and regulatory requirements.

2.3 Regulatory Compliance

This Policy and associated documentation are aligned with applicable legal and regulatory frameworks, including data protection, commercial communications, marketing, intellectual property and other relevant areas.

2.4 Resource Allocation

GORLAN's Management is committed to providing the necessary resources to implement, maintain and continuously improve information security processes and ensure compliance with this Policy.

3. Responsibilities

3.1 Roles and Responsibilities

All users affected by this Policy must comply with it, actively protect information, maintain confidentiality, and report any suspected security incidents or vulnerabilities.

3.2 Chief Information Security Officer (CISO)

The CISO ensures that the Information Security Policy and ISMS are established and implemented to protect the organisation's information assets.

3.3 Service Owner

The Service Owner oversees operational and strategic aspects of service security and ensures regulatory compliance.

3.4 Information Owner

The Information Owner ensures proper protection, classification and integrity of information throughout its lifecycle.

3.5 System Owner

The System Owner ensures that information systems meet established security requirements and are properly maintained.

3.6 Security Committee

GORLAN has a Security Committee responsible for aligning security activities across the organisation, including physical security, information security, compliance and contingency planning.

4. References

ISO/IEC 27001:2022

ISO/IEC 27002:2022

Regulation (EU) 2016/679 (GDPR)

Organic Law 3/2018 (LOPDGDD)

5. Modification Control

Edition.Revision	Date	Description
00.00	2025-03-24	Policy Approval