



GYALA
Cyber security

Quality and Information Security Policy

—

POL_PQU Rev. 3

PUBLIC

Revision history

Date	Description	Chapters/Paragraphs changed	Review
01/02/2019	First Issue	All	0
30/06/2022	Integration 27001	All	1
11/04/2023	General Review	All	2
11/09/2024	Adaptation to ISO/IEC 27001:2022	All	3

Note changes from the previous version are marked with sidebars.

Approval

Role	Name	Sign	Date
Editor(s) Reviewer(s)	Gian Roberto Sfoglietta – CEO		11/09/2024
	Nicola Mugnato – Cheaf Technical Officer		
	Luca Colamedici – System Manager		
Approver	Gian Roberto Sfoglietta – CEO		11/09/2024

Questo documento contiene informazioni riservate di proprietà esclusiva della società Gyala s.r.l. Tutte le informazioni in esso contenute non potranno essere pubblicate, riprodotte, copiate, divulgate o usate per altri scopi diversi da quelle di cui al presente documento, senza autorizzazione scritta da parte di un rappresentante legale di questa società.

Index

1.	PURPOSE AND SCOPE.....	4
2.	REFERENCES.....	4
3.	QUALITY AT GYALA.....	5
3.1.	WHO WE ARE.....	5
3.2.	VISION.....	6
4.	OBJECTIVES FRAMEWORK.....	6
5.	INFORMATION SECURITY COMMITMENTS – ISO/IEC 27001.....	7

1. PURPOSE AND SCOPE

This Policy outlines the guidelines and principles established by Gyala S.r.l.'s management regarding Quality and Information Security within the company's Management System, in accordance with ISO 9001:2015 and ISO/IEC 27001:2022 standards. This Policy is shared within the organization and made available to interested parties through publication on the company website. The contents of this Policy are reviewed periodically to ensure they remain current and appropriate to the company's goals and context.

2. REFERENCES

ID	Document Title
ISO 9001:2015	Quality Management Systems – Requirements
ISO 9000:2015	Quality Management Systems – Fundamentals and Vocabulary
ISO/IEC 27001:2022	Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements
ISO/IEC 27002:2022	Information Security, Cybersecurity and Privacy Protection – Information Security Controls

3. QUALITY AT GYALA

3.1. Who We Are

Gyala is a fully Italian-owned company specializing in cybersecurity software systems. Founded in 2017 by three co-founders with twenty years of experience in defense, IT, and security, Gyala has developed a technological platform for cyber incident detection and reaction called Agger. Initially co-funded by the National Military Research Program (PNRM), Agger has been successfully tested by both the Italian Army Cyber Unit and the Italian Navy.

Today, Agger is a modular, scalable, AI-based platform adaptable to any infrastructure. It provides advanced protection capabilities for IT and OT environments, either through automated reactions or by guiding non-expert operators with clear operational procedures.

Agger addresses the shortage of highly specialized professionals and reduces Security Operation Center (SOC) costs by eliminating the need for constant human monitoring. It enables uniform and comprehensive detection and incident management across both IT and industrial OT infrastructure.

The Agger source code was developed entirely in Italy by Italian experts, with the explicit goal of creating a system capable of monitoring all network communications and process behavior to detect anomalies—including hidden behavior from foreign hardware, firmware, or OS suppliers.

Originally developed for the defense sector, the platform has since 2020 been deployed in critical infrastructures (power plants, hospitals) and industrial companies. A simplified version for SMEs, named Uranyo, has also been developed.

Gyala continues to invest in research and development to expand the capabilities and applications of its products. Collaborations with universities and defense experts, including further PNRM-funded projects like CYMON (focused on cyber threat detection in avionics networks), underscore its innovation strategy.

To support its growth, Gyala has opened its capital to exclusively Italian investors. A recent funding round was led by CDP Venture Capital (via the Evoluzione Fund), alongside Azimut Libera Impresa and Italian Angels for Growth (IAG).

3.2. Vision

At Gyala, customer satisfaction is a core objective. The company organizes its activities to ensure quality and timely delivery, always in full compliance with customer and regulatory requirements.

These core values are shared across the organization to foster alignment with business goals.

The Integrated Quality and Information Security Management System, compliant with ISO 9001:2015 and ISO/IEC 27001:2022, is considered a strategic asset to ensure consistent delivery of products and services and to enhance customer satisfaction. Gyala is committed to meeting all applicable requirements and to continuously improving its Integrated Management System.

4. OBJECTIVE FRAMEWORK

Gyala defines the following objectives for its Quality and Information Security strategy:

<i>Area</i>	<i>No.</i>	<i>Objective</i>
Sales	1	Understand customer needs and respond promptly with innovative, secure, and tailored solutions.
Software Solutions	2	Ensure timely delivery of compliant and secure solutions.
	3	Flexibly respond to evolving customer needs during the design and development lifecycle, while maintaining defined security requirements.
Consulting Services	4	Provide high-level, specialized consulting with flexibility and punctuality, ensuring information security throughout the service lifecycle.

5. INFORMATION SECURITY COMMITMENTS – ISO/IEC 27001

Gyala is committed to complying with applicable legal and regulatory requirements, particularly ISO/IEC 27001, and to ensuring that:

- Information is protected from unauthorized access, ensuring confidentiality and availability to authorized users;
- Information is not disclosed to unauthorized individuals, whether by negligence or intent, and that integrity is preserved by preventing unauthorized modifications;
- Business continuity plans are in place, kept up to date, and tested regularly;
- Personnel receive training on information security;
- All information security incidents and vulnerabilities are reported, reviewed, and addressed.

By implementing this policy, Gyala affirms its commitment to ISO/IEC 27001 compliance.

The management ensures this Policy is communicated, understood, and applied not only by internal staff but also by external collaborators, consultants, and suppliers who handle information within the scope of the Information Security Management System.

The management also commits to regularly reviewing the Policy and any influencing changes to ensure it remains relevant and aligned with Gyala's ability to meet the expectations of customers, suppliers, partners, and all interested parties.