

# Politica del Sistema di Gestione Integrato

## ISO 9001 – ISO 27001 – ISO 27017

<i>Authors:</i>	Gianmarco Piras, Massimiliano Gimondo
<i>Approver:</i>	Dario Sabella
Confidentiality level	PU - Public
Status	Approved
Version:	1.0.0
Date	Torino, 09/03/2026



## TABLE OF CONTENTS

1	Scopo, Visione e Campo di Applicazione .....	3
2	Impegni Fondamentali della Direzione (Requisiti ISO 9001 e ISO 27001) .....	3
3	Eccellenza Operativa e Gestione della Qualità (ISO 9001) .....	3
4	Tutela del Patrimonio Informativo e Gestione degli Incidenti (ISO/IEC 27001) .....	4
5	Sicurezza in Ambito Cloud e Infrastrutturale (ISO/IEC 27017) .....	4
6	Conformità Normativa e Trattamento dei Dati Personali .....	4
7	Comunicazione, Condivisione e Cultura Aziendale .....	4
8	Bibliografia .....	5

## 1 Scopo, Visione e Campo di Applicazione

La presente Politica del Sistema di Gestione Integrato (SGI) definisce la visione strategica, le direttive operative e gli impegni formali assunti dall'Alta Direzione di Next G Cloud (NGC) in materia di Gestione della Qualità (ISO 9001), Sicurezza delle Informazioni (ISO/IEC 27001) e Sicurezza dei Servizi Cloud (ISO/IEC 27017). Il documento si applica in modo trasversale e vincolante a tutto il personale aziendale (dipendenti, collaboratori, consulenti, tirocinanti), estendendosi ai fornitori, ai partner e a tutti i processi legati all'erogazione dei servizi cloud. La visione di Next G Cloud è consolidarsi come punto di riferimento autorevole e innovativo nel panorama europeo; a tal fine, l'azienda partecipa attivamente alla standardizzazione internazionale (es. ETSI) e collabora tramite le proprie divisioni di Ricerca e Sviluppo (R&D) con governi ed enti dell'Unione Europea per il co-sviluppo di soluzioni sicure e interoperabili.

## 2 Impegni Fondamentali della Direzione (Requisiti ISO 9001 e ISO 27001)

Per tradurre la propria visione in risultati tangibili, l'Alta Direzione di Next G Cloud si assume la responsabilità dell'efficacia del Sistema di Gestione Integrato e si impegna formalmente a:

- Soddisfare tutti i requisiti applicabili, siano essi di natura cogente (leggi e regolamenti), normativa, contrattuale (SLA con i clienti) o legati alla sicurezza delle informazioni e alla privacy.
- Migliorare continuamente l'efficacia, l'efficienza e le prestazioni del Sistema di Gestione Integrato, adattandolo costantemente all'evoluzione del contesto interno ed esterno e alle nuove minacce.
- Fornire un quadro di riferimento strutturato per la definizione, il monitoraggio e il riesame degli obiettivi di qualità e di sicurezza delle informazioni, garantendo che tali traguardi siano misurabili e coerenti con gli indirizzi strategici dell'azienda.

## 3 Eccellenza Operativa e Gestione della Qualità (ISO 9001)

L'obiettivo primario di Next G Cloud è massimizzare la soddisfazione del cliente attraverso l'erogazione di servizi cloud e architetture che rispondano rigorosamente alle aspettative. Per assicurare questo standard, l'azienda ha adottato un approccio metodologico basato su framework Agile e Scrum, integrando la qualità direttamente nel ciclo di vita dello sviluppo software (SDLC). Durante la pianificazione di ogni progetto vengono stabiliti i requisiti funzionali e non funzionali, garantendo che il rilascio finale sia preceduto da controlli rigorosi quali review di progetto, test intermedi, revisioni paritarie del codice (Code Review) e analisi statica (SAST).

Inoltre, l'azienda stabilisce obiettivi per la qualità misurabili e coerenti con la politica. Gli obiettivi sono definiti annualmente durante il Riesame della Direzione e monitorati trimestralmente (supportati anche dalla metodologia OKR implementata in azienda per il goal setting).

## 4 Tutela del Patrimonio Informativo e Gestione degli Incidenti (ISO/IEC 27001)

La protezione della riservatezza, dell'integrità e della disponibilità (CIA) dei dati rappresenta il fulcro operativo di Next G Cloud. L'organizzazione applica il principio del "Secure by Design" per difendere i propri asset strategici, la proprietà intellettuale e le informazioni dei clienti da minacce di ogni natura. È stato istituito un rigoroso processo di gestione degli incidenti: in caso di violazione dei dati (Data Breach), l'azienda garantisce la notifica al Garante della Privacy entro 72 ore tramite il coordinamento del DPO e del CISO. Per fronteggiare attacchi severi (es. ransomware), le procedure prevedono la notifica al CSIRT entro 6 ore, sotto la supervisione dell'Escalation Manager. La sicurezza è garantita anche dalla continua formazione del personale, erogata tramite Internal Training, newsletter bimensili e simulazioni anti-phishing basate sui ruoli (piattaforma RIOT).

## 5 Sicurezza in Ambito Cloud e Infrastrutturale (ISO/IEC 27017)

L'erogazione dei servizi cloud poggia su infrastrutture progettate per garantire massima resilienza e sicurezza perimetrale. I server centrali sono ospitati esclusivamente presso Data Center certificati Tier IV (es. Aruba), mentre l'accesso ai siti sperimentali è severamente normato da specifici Memorandum of Understanding (MOU). A livello logico, tutte le comunicazioni e i trasferimenti di dati (Data in Transit) avvengono tramite protocolli crittografici sicuri (TLS 1.3 o superiori, VPN). L'azienda vieta categoricamente l'uso di servizi cloud non autorizzati (Shadow IT) e protegge l'infrastruttura di Lavoro Agile (Smart Working) mediante la fornitura ai propri dipendenti di PC aziendali dotati di antivirus aziendale.

## 6 Conformità Normativa e Trattamento dei Dati Personali

La Direzione garantisce il pieno allineamento alle cogenze legali. La protezione dei dati personali è gestita in stretta conformità con il GDPR (Reg. UE 679/16) e il D.Lgs. 196/2003 e smi: ogni nuovo servizio o tecnologia (es. Intelligenza Artificiale) è soggetto a Valutazione d'Impatto (DPIA) e alla stipula di accordi sul trattamento dei dati (DPA). L'azienda assicura altresì il rispetto della Direttiva NIS2 sulla cybersicurezza, del D.Lgs. 81/08 per la sicurezza sul lavoro e della Legge 128/2004 sul diritto d'autore. La riservatezza con i soggetti terzi è sistematicamente tutelata tramite Accordi di Non Divulgazione (NDA) rigorosi.

## 7 Comunicazione, Condivisione e Cultura Aziendale

Affinché questa politica sia efficace, la Direzione assicura che essa sia disponibile come informazione documentata, mantenuta aggiornata e resa accessibile a tutte le parti interessate rilevanti. Il documento viene formalmente comunicato, compreso e applicato all'interno dell'organizzazione: il suo rispetto è vincolante fin dalla fase di onboarding tramite l'accettazione del Regolamento Interno (Employee Handbook). A garanzia della trasparenza e del

miglioramento del sistema, i Responsabili di Linea vigilano sulla corretta applicazione delle policy, supportati da un canale di Whistleblowing (su SharePoint) per la segnalazione protetta di non conformità. L'efficacia del SGI viene inoltre valutata sistematicamente tramite audit interni indipendenti e verifiche di terza parte.

## 8 Bibliografia

- [1] ISO 9001:2015 – Sistemi di gestione per la Qualità – Requisiti
- [2] ISO/IEC 27001:2022 c Sicurezza delle informazioni, cybersecurity e protezione della privacy – Sistemi di gestione per la sicurezza delle informazioni – Requisiti
- [2] ISO/IEC 27002:2023 - Sicurezza delle informazioni, cybersecurity e protezione della privacy - Controlli di sicurezza delle informazioni
- [3] ISO/IEC 27017:2021 – Tecnologie Informatiche - Tecniche di sicurezza - Raccolta di prassi sui controlli per la sicurezza delle informazioni per i servizi in cloud basata sulla ISO/IEC 27002

## DOCUMENT HISTORY

Date	Version	Author	Comments
06/03/2026	0.1	Gianmarco Piras	First version
09/03/2026	1.0	Dario Sabella	Approved

**NEXT G CLOUD** is a cutting-edge technology company specializing in managed cloud services, advanced training and strategic consultancy.

Leveraging the latest advancements in edge computing, artificial intelligence and quantum technologies, we offer unique solutions to secure infrastructures and applications for developers and enterprises

[www.nextgcloud.com](http://www.nextgcloud.com)

