



Politica Sistema Integrato

	Politica Sistema Integrato	PO 5.2	
		Rev. 2.0	09/07/2025
		Pag 2 di 10	

Revisioni

Rev.	Data	Descrizione	Redatto	Approvato
0.0	05/02/2021	Prima emissione	Riccardo Ottonello	CdA
1.0	08/07/2024	Revisione Brand Revisione per transizione alla nuova norma ISO27001:2022	Riccardo Ottonello	CdA
2.0	09/07/2025	Revisione per recepimento ed integrazione con nuova norma ISO9001:2015	Pamela Pentimalli	CdA

	Politica Sistema Integrato	PO 5.2	
		Rev. 2.0	09/07/2025
		Pag 3 di 10	

Indice

Revisioni	2
Indice	3
1 Introduzione	4
1.1 Scopo	4
1.2 Campo di applicazione	4
1.3 Riferimenti e Allegati	4
1.4 Definizioni, Acronimi, Abbreviazioni	4
1.5 Responsabilità	5
1.6 Riesame	6
2 Impostazione della Politica	6
3 Politica per la Sicurezza delle informazioni e la Protezione dei dati personali	6
4 Ambito di Applicazione	9
5 Violazione della Politica	9

	Politica Sistema Integrato		PO 5.2
			Rev. 2.0 09/07/2025
	Pag 4 di 10		

1 Introduzione

1.1 Scopo

La presente Politica è utilizzata come strumento per sensibilizzare l'intera organizzazione sui principi di Sicurezza delle Informazioni aziendali, qualità e protezione dei Dati personali e viene applicata in tutti gli ambiti specificati nel perimetro di certificazione nonché a tutto il personale di Wildcard service s.r.l. (di seguito definita anche come "Wildcard", "l'Organizzazione" o "l'Azienda"), ai clienti, ai fornitori che siano in qualche modo coinvolti nel trattamento di informazioni e dei dati personali che rientrano nel campo di applicazione del Sistema di Gestione Integrato.

1.2 Campo di applicazione

La presente politica si applica a tutti gli ambiti aziendali, a tutto il personale aziendale coinvolto nel campo di applicazione del Sistema di Gestione (vedi capitolo 5) e a tutti gli stakeholder identificati nel contesto (vedi paragrafo 3.1). Tale documento è pertanto rivolto ai seguenti destinatari:

- dipendenti;
- clienti;
- fornitori;
- partner commerciali.

1.3 Riferimenti e Allegati

AL 5.3.A - Organigramma Wildcard

ISO/IEC 27001:2022- Sicurezza delle informazioni, cybersecurity e protezione della privacy -

Requisiti

ISO 9001:2015 - Sistemi di gestione per la qualità - Requisiti

RDGP / GDPR - Regolamento Generale sulla Protezione dei Dati.

1.4 Definizioni, Acronimi, Abbreviazioni

CDA – Consiglio di Amministrazione

CEO - Chief Executive Officer

DPO – Data Protection Officer

	Politica Sistema Integrato		PO 5.2
			Rev. 2.0 09/07/2025
	Pag 5 di 10		

RSGI - Responsabile del Sistema di Gestione Integrato

SGI - Sistema di Gestione Integrato (Sicurezza delle Informazioni e Protezione dei dati personali)

SGSI - Sistema di Gestione della Sicurezza delle Informazioni.

1.5 Responsabilità

La Direzione ha la responsabilità di redigere, mantenere aggiornata e comunicare la presente politica. La Direzione, ha il compito di definirne l'ambito del sistema di gestione, attivarsi per il miglioramento e controllare l'applicazione.

Il personale, a qualsiasi livello, e i collaboratori esterni devono attenersi alle procedure definite dall'Organizzazione per assicurarsi che la presente Politica sia correttamente applicata.

L'organigramma è definito in "*AL 5.3.A – Organigramma Wildcard*".

I responsabili dell'attuazione della presente politica sono:

- la Direzione di Wildcard, che stabilisce i criteri di accettazione e i livelli di accettabilità del rischio, fornisce le risorse necessarie per garantire la corretta applicazione della sicurezza delle informazioni e protezione dei dati personali, assicura lo svolgimento di audit interni e garantisce il pieno supporto nell'attuazione della presente politica, affidando alle diverse funzioni compiti di implementazione, gestione e monitoraggio dell'efficacia ed efficienza del sistema. All'interno di ogni funzione è stabilita la definizione degli opportuni ruoli e responsabilità per la gestione della sicurezza dell'informazione e gestione del servizio,
- il RSGI, che facilita l'attuazione della presente politica attraverso norme e procedure appropriate,
- tutto il personale di Wildcard, a cui sono assegnati precisi ruoli e responsabilità. Esso deve avere un'adeguata competenza per svolgere i compiti richiesti, pertanto deve essere informato e formato adeguatamente riguardo agli obiettivi dell'azienda in tema di sicurezza e protezione dei dati personali. Sono definite e mantenute registrazioni sull'istruzione, formazione, abilità, esperienze e qualifiche. Tutto il personale ha la responsabilità di reagire tempestivamente agli incidenti contro la sicurezza e/o non conformità del prodotto/servizio e a segnalare al RSGI qualsiasi punto debole individuato nel sistema,
- Clienti e Fornitori coinvolti nella gestione dei prodotti/servizi implementati, che rientrano nel perimetro di applicazione del SGI. Essi sono tenuti al rispetto della Politica di Wildcard per garantire la sicurezza delle informazioni trattate e la protezione dei dati personali.



1.6 Riesame

La revisione di tale politica è effettuata dalla Direzione almeno una volta all'anno e prima del Riesame della direzione, e in risposta a cambiamenti significativi dell'ambiente organizzativo, del business, di riferimenti normativi o dell'ambiente tecnologico aziendale. Il riesame è condotto per valutare l'efficienza e l'efficacia del sistema e per assicurare che siano poste in essere le azioni necessarie per consentire il miglioramento continuo secondo i requisiti definiti dai sistemi di gestione e in tutte le situazioni per le quali è richiesta una modifica dell'attività aziendale che possa anche avere impatto sulla sicurezza delle informazioni o sull'operatività.

2 Impostazione della Politica

Wildcard percepisce come necessità di crescita aziendale la sempre maggiore diffusione della cultura della sicurezza al suo interno, e pertanto ha assunto un ruolo attivo e operativo nelle attività di impostazione e di implementazione di un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) anche a supporto della protezione dei dati personali secondo il regolamento europeo GDPR. La Direzione definisce quindi in maniera chiara e puntuale la Politica che l'Azienda intende perseguire, dandone specifica relazione ai rischi, alle minacce e alle vulnerabilità, tenendo conto del tipo di business esercitato.

3 Politica per la Qualità e la Sicurezza delle informazioni e la Protezione dei dati personali

Wildcard si impegna ad attuare un sistema di gestione integrato per la qualità e la sicurezza delle informazioni documentate, lo sviluppo dell'attività, la gestione dei costi e dei rischi, il miglioramento continuo della soddisfazione dei Clienti e del personale dell'Organizzazione, la protezione da minacce, interne o esterne, intenzionali o accidentali, del patrimonio informativo aziendale e a svolgere attività di business nel pieno rispetto della Sicurezza delle Informazioni.

Wildcard si impegna ad attuare, implementare, gestire, monitorare, revisionare, mantenere e migliorare il sistema di gestione per la Qualità, in conformità alla Norma ISO9001:2015, e per la Sicurezza delle Informazioni e Protezione dei dati personali, in conformità alla Norma ISO/IEC 27001:2022 e GDPR.

Con l'attuazione della presente politica, Wildcard garantisce ai propri Clienti la qualità dei propri prodotti, nel rispetto della sicurezza delle informazioni.

	Politica Sistema Integrato		PO 5.2
			Rev. 2.0 09/07/2025
	Pag 7 di 10		

Wildcard si impegna ad adempiere agli obblighi di adeguamento al Regolamento Generale sulla Protezione dei Dati (GDPR) direttamente applicabile a partire da 25 Maggio 2018, attraverso

- l'elaborazione del registro delle attività di trattamento (sia come Titolare del Trattamento che Responsabile esterno);
- la valutazione d'impatto sulla protezione dei dati, laddove applicabile;
- l'applicazione di misure tecniche ed organizzative adeguate intese a garantire la sicurezza dei dati e derivanti da un processo di analisi del rischio;
- designazione di un Responsabile della Protezione dei Dati (Data Protection Officer)
- definizione all'interno (e se necessario all'esterno) dell'azienda di ruoli e responsabilità relativi al trattamento dei dati.

Wildcard si impegna ad attenersi ai principi di protezione dei dati contenuti nel GDPR per garantire che tutti i dati siano:

- trattati dimostrando l'accountability, nel rispetto dei principi di privacy by design e by default;
- trattati in modo lecito, corretto e trasparente;
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che siano compatibili con tali finalità;
- adeguati, pertinenti e non sovrabbondanti;
- accurati e mantenuti aggiornati;
- conservati per il tempo necessario;
- trattati in conformità dei diritti dell'interessato;
- sicuri;
- non trasferiti all'estero senza adeguata protezione.

Sono state stabilite le responsabilità generali del Titolare del trattamento nella figura del Legale Rappresentante (membri del CDA) per qualsiasi trattamento di dati personali che effettui direttamente o che altri effettuino per suo conto. In particolare, Wildcard mette in atto misure adeguate ed efficaci, così da essere in grado di dimostrare la conformità delle attività di trattamento con il GDPR, compresa l'efficacia delle misure, che tengono conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.

È scopo di Wildcard assicurare di:

- orientare i propri obiettivi e le strategie operative partendo da un'attenta analisi del contesto (interno ed esterno), delle parti interessate e dei rischi rilevati;
- ottenere e mantenere la Certificazione di Qualità ISO 9001:2015;



Politica Sistema Integrato

PO 5.2

Rev. 2.0

09/07/2025

Pag 8 di 10

- garantire la conformità alle leggi e ai regolamenti applicabili alle attività e ai servizi di Wildcard;
- stabilire efficaci modalità di gestione e di controllo;
- perseguire il miglioramento continuo dell'Organizzazione attraverso il monitoraggio dei risultati delle attività e la verifica dell'efficienza dei processi;
- monitorare e perseguire il miglioramento continuo della soddisfazione dei Clienti, tramite la realizzazione di prodotti e servizi di qualità, conformi alle loro aspettative e ai requisiti di legge.
- sviluppare azioni di aggiornamento continuo per i propri dipendenti e collaboratori interni, promuovendone lo sviluppo professionale, la motivazione e la migliore assimilazione possibile del Sistema di Gestione per la Qualità, anche al fine di creare un ambiente adatto al pieno coinvolgimento e alla motivazione del personale nel perseguimento degli obiettivi;
- gestire i rapporti con i propri fornitori in un'ottica di reciproco beneficio al fine di migliorare le capacità di entrambi di creare valore;
- sostenere, diffondere e rendere comprensibile a tutto il personale aziendale la Politica del Sistema di Gestione della Qualità, distribuendo alle funzioni aziendali interessate la documentazione riguardante gli specifici compiti a esse assegnati e promuovendo opportune azioni di formazione e comunicazione mediante gli strumenti aziendali in essere;
- diffondere all'esterno (clienti / fornitori) la politica del Sistema di Gestione della Qualità, attraverso il sito internet aziendale;
- far perseguire al personale aziendale la politica stabilita, gli obiettivi periodicamente loro assegnati, mettendo a disposizione le risorse e i mezzi necessari;
- provvedere periodicamente alla verifica dell'attuazione della politica durante gli audit interni;
- procedere al Riesame sistematico della continua idoneità dei suoi contenuti, ai fini dell'ottenimento dei requisiti e del miglioramento continuativo del Sistema di Gestione della Qualità;
- rispettare tutte le prescrizioni cogenti legate al settore di riferimento, agli effetti che l'azienda ha sull'ambiente, ai contratti di lavoro ed ai diritti dei lavoratori;
- mantenere la Certificazione ISO/IEC 27001:2022 -Sistemi di gestione per la sicurezza delle informazioni - Requisiti
- le informazioni siano protette da accessi non autorizzati e non vengano divulgate a persone non autorizzate;
- vengano definiti programmi formativi di dettaglio sulla Sicurezza delle Informazioni e sulla Protezione dei Dati personali per tutti i dipendenti interni e per tutto il personale esterno che opera per prolungati periodi all'interno dell'organizzazione qualora si verificasse quest'ultima eventualità;



- l'integrità delle informazioni sia protetta e salvaguardata da modifiche non autorizzate;
- venga definita, documentata e riesaminata periodicamente una procedura per il controllo degli accessi alle informazioni basata sui requisiti per l'accesso relativi alla sicurezza e all'attività dell'Azienda, dettagliando in base a accessi fisici e accessi logici;
- venga definita e documentata la procedura per la comunicazione tempestiva e per la gestione degli incidenti in caso di minaccia alla sicurezza dell'informazione in particolar modo quando questi coinvolgano dati personali (Data Breach). Siano pertanto immediatamente riconoscibili i responsabili e le azioni correttive da intraprendere;
- le informazioni siano a disposizione degli utenti autorizzati quando ne hanno bisogno;
- vengano redatti piani per la continuità dell'attività aziendale, e che tali piani siano il più possibile tenuti aggiornati e controllati;
- quando è concesso l'accesso alle informazioni o agli asset dell'Organizzazione da parte di terzi vengano attuati controlli appropriati prima di concedere l'accesso.

4 Ambito di Applicazione

L'obiettivo di Wildcard è quello di certificare l'azienda in materia di sicurezza delle informazioni e qualità, in quanto ritiene che questo possa essere di supporto al business e quindi al raggiungimento degli obiettivi strategici. La Direzione ha definito il seguente ambito di certificazione:

"Progettazione, sviluppo, realizzazione ed assistenza di soluzioni informatiche e telematiche, reti, integrazione di sistemi ICT, System and Network Management, infrastrutture virtualizzate, sistemi IoT, VoIP, videoconferenza, videosorveglianza, backup remoti, Disaster Recovery e Business Continuity. Assistenza tecnica con HelpDesk, gestione Incident, Problem Management. Gestione di sistemi informatici On-Premise, in Housing, Hosting e Outsourcing, erogazione servizi Cloud in modalità IaaS e PaaS, conduzione Server Farm, inclusi i servizi NOC (Networking Operation Center) e SOC (Security Operation Center), monitoraggio di rete e dei sistemi, erogazione di connettività Internet filtrata. Erogazione di servizi di CyberSecurity. Fornitura di Software e Hardware".

5 Violazione della Politica

Qualsiasi azione non conforme alla politica aziendale dell'Organizzazione sarà considerata una violazione della sicurezza e come tale si tradurrà nella revoca dell'accesso alle aree e alle risorse informatiche, rete e documenti. L'uso improprio degli strumenti aziendali costituisce una grave violazione del dovere di correttezza e può comportare l'adozione di provvedimenti disciplinari in conformità alla normativa vigente.

	Politica Sistema Integrato		PO 5.2	
			Rev. 2.0	09/07/2025
	Pag 10 di 10			

I casi gravi saranno segnalati all'autorità competente e potranno essere oggetto di provvedimenti disciplinari o legali.