Politica per la Sicurezza delle Informazioni e Protezione dei Dati Personali

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

Indice

1 Introduzione

1.1 Scopo

La presente Politica è utilizzata come strumento per sensibilizzare l'intera organizzazione sui principi di Sicurezza delle Informazioni aziendali 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.

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
AL 4.1.A - Diagramma Contesto
AL 4.1.B - Analisi Stakeholder
ISO/IEC 27001:2022- Sistemi di gestione per la sicurezza delle informazioni – 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
RSGI - Responsabile del Sistema di Gestione Integrato
SGI - Sistema di Gestione Integrato (Sicurezza delle Informazione 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.

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 Wildcard

Wildcard è nata nel 1998 con lo scopo di proporsi come partner tecnologico di imprese ed organizzazioni complesse. Nel corso degli anni ha sviluppato competenze specifiche nell'integrazione di sistemi informatici.

Il suo business si muove principalmente su tre aree:

- consulenza
- erogazione di servizi
- vendita di hardware

L'analisi degli Stakeholder interni ed esterni di Wildcard è illustrata in dettaglio nell'Allegato "*AL 4.1.B – Analisi Stakeholder*".

3.1 Contesto

L'Organizzazione ha identificato il contesto in termini di siti fisici, ambienti cloud, stakeholder afferenti al sistema di gestione e ha mappato i processi aziendali sia di core business che di supporto in documento "*AL 4.1.A – Diagramma Contesto*".

Un'analisi specifica viene effettuata per comprendere quali possano essere le implicazioni dei cambiamenti climatici sull'operatività aziendale: da un lato, Wildcard è un'azienda di servizi e, come tale, ha un impatto ambientale ridotto, equiparabile a tradizionali uffici e non a fabbriche; dall'altro, opera in un contesto ambientale nel quale il clima è temperato, ma il territorio è considerato potenzialmente soggetto ad alluvioni e la sede si trova nelle vicinanze di un fiume che ha caratteristiche torrentizie (Polcevera); tuttavia, l'ufficio si trova ad un piano alto ed è stato definito un apposito piano per la continuità operativa in caso di indisponibilità della sede per eventi avversi esterni (vedere "*MD A 5.29.A - Piani di Continuità Operativa_Indisponibilità sede eventi avversi esterni ID-PBC05*") e/o un piano per la possibile mancanza di elettricità (vedere "*MD A 5.29.A - Piani di Continuità Operativa_Mancanza elettricità sede ID-PBC08*"). La sede non si trova in zona ritenuta sismicamente a rischio.

Il contesto in cui si colloca la server farm a Trento offre garanzie non inferiori a quelle dell'ufficio di Genova, trattandosi di un ambiente professionale di erogazione servizi Data Center gestito da un provider a sua volta dotato delle idonee certificazioni, anche ambientali: https://irideos.it/certificazioni/ . La sede non si trova in zona ritenuta sismicamente a rischio. La sede si trova nelle vicinanze del fiume Adige, tuttavia il Data Center è dotato di tutte le misure idonee per il mantenimento dell'alimentazione elettrica in caso di disservizio per evento di allagamento. I server si trovano su piano rialzato rispetto al fondo, e quindi in zona a basso rischio di allagamento anche in caso di tracimazione dagli argini (evento che comunque si ritiene tuttora a probabilità di accadimento molto bassa).

Il fornitore dei servizi in Data Center, inoltre, è certificato ISO14001 e con piano di sostenibilità ambientale descritto su https://www.retelit.it/it/sostenibilita , con impegno a diventare azienda Net-Zero entro il 2050.

A fronte di tali considerazioni, si può sostenere che anche gli stakeholders esterni non nutrono preoccupazioni nei confronti dell'operatività di Wildcard, la quale garantisce la continuità dei propri servizi.

L'organigramma è definito in "*AL 5.3.A – Organigramma Wildcard*" e riflette la struttura dei processi sotto mostrati.

4 Politica per la Sicurezza delle informazioni e la Protezione dei dati personali

Wildcard si impegna a proteggere da minacce, interne o esterne, intenzionali o accidentali, il 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 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 prodotti sicuri nel rispetto della sicurezza delle informazioni.
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 che:

- 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.

5 Ambito di Applicazione

L'obiettivo di Wildcard è quello di certificare l'azienda in materia di sicurezza delle informazioni, 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".

6 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.
I casi gravi saranno segnalati all'autorità competente e potranno essere oggetto di provvedimenti disciplinari o legali.