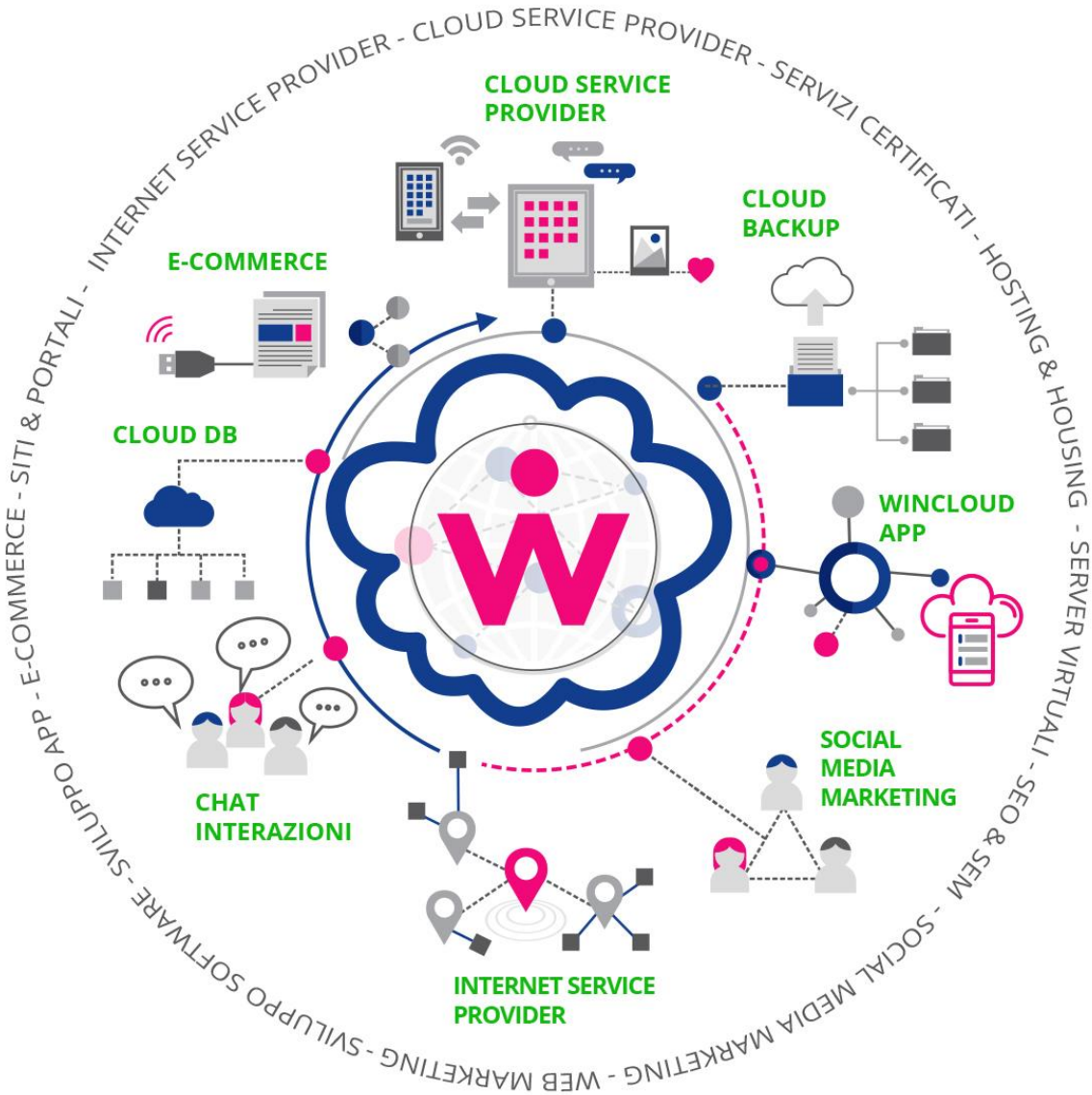


Emesso da: Arch. Floriana Venturucci _____

Politica per la sicurezza delle informazioni

WIN S.r.l. - Wineuropa.it è azienda di Internet Service Provider dal 1999 operante nel settore.

La rete è il mezzo attraverso il quale si sviluppa il business, conseguentemente per il business è vitale disporre di un sistema di sicurezza delle informazioni.

Oltre al rispetto dei requisiti relativi alla protezione dei dati personali previsti dal Regolamento (UE) 2016/679 (GDPR) e dalla normativa nazionale applicabile, WIN S.r.l. - Wineuropa.it ha adottato un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) certificato in conformità alla UNI CEI EN ISO/IEC 27001. Il SGSI è mantenuto e migliorato attraverso audit interni, audit di terza parte, monitoraggio degli obiettivi e Riesame della Direzione, tenendo conto della versione vigente della norma e dei requisiti applicabili.

La Direzione assicura che il SGSI sia coerente con il contesto, la strategia e il perimetro dei servizi aziendali, tenendo conto delle esigenze delle Parti Interessate, dei requisiti legali, regolamentari e contrattuali e dei fattori interni ed esterni rilevanti, inclusi, ove pertinenti, quelli ambientali e climatici. La presente Politica costituisce il quadro di riferimento per la definizione e il riesame di obiettivi di sicurezza misurabili e per il miglioramento continuo del SGSI.

WIN S.r.l. mantiene aggiornato il quadro dei requisiti cogenti applicabili. Ove ricorrano i presupposti di applicazione, sono recepiti anche gli obblighi previsti dal D.Lgs. 4 settembre 2024, n. 138 di recepimento della Direttiva (UE) 2022/2555 (NIS2), nonché dalle determinazioni e indicazioni dell'Agenzia per la Cybersicurezza Nazionale (ACN) e dalle eventuali norme settoriali pertinenti.

Dal 1999 siamo Registrar accreditati presso il nic.it il Registro Italiano dei nomi a dominio.

Le tecnologie e i servizi di sicurezza sono selezionati sulla base di requisiti tecnici, valutazioni del rischio, affidabilità dei fornitori e stato dell'arte; la loro adeguatezza è riesaminata periodicamente e non dipende dall'adozione di uno specifico marchio o prodotto.

I servizi esposti su reti pubbliche utilizzano protocolli crittografici e certificati digitali emessi da Certification Authority attendibili; emissione, rinnovo, revoca, configurazione e scadenza dei certificati sono gestiti secondo procedure definite (tutto rintracciabile sulla dashboard).

Con l'implementazione del SGSI WIN S.r.l. - Wineuropa.it intende proteggere le informazioni e i servizi in modo proporzionato ai rischi, soddisfare i requisiti applicabili e tutelare gli interessi dell'organizzazione, dei clienti e delle altre Parti Interessate.

WIN S.r.l. - Wineuropa.it effettua sistematicamente la gestione del rischio di sicurezza delle informazioni mediante criteri definiti di identificazione, analisi, valutazione, trattamento, accettazione del rischio residuo e monitoraggio. I rischi sono associati a responsabili, misure di trattamento, priorità e tempi di attuazione e sono riesaminati periodicamente e in occasione di cambiamenti significativi, nuovi servizi, incidenti rilevanti o variazioni del contesto.

La gestione del rischio adotta un approccio "all-hazards" che considera, in modo proporzionato, minacce informatiche, errore umano, guasti tecnologici, eventi fisici e ambientali, indisponibilità di servizi o fornitori e altri scenari rilevanti per la continuità e la resilienza dei servizi.

Il quadro strategico di riferimento degli obiettivi è determinato sulla base della qualità, della sicurezza e della resilienza dei servizi, con particolare attenzione a riservatezza, integrità, disponibilità e, ove applicabile, autenticità delle informazioni e dei sistemi.

La qualità e la sicurezza del servizio sono definite mediante parametri prestazionali e obiettivi misurabili, con responsabilità, indicatori, valori attesi e frequenze di verifica definiti, monitorati e riesaminati dalla Direzione in coerenza con le strategie aziendali.

Gli esiti del monitoraggio, degli audit, degli incidenti, delle verifiche di vulnerabilità, delle prove di continuità e delle valutazioni dei fornitori sono analizzati per verificare l'efficacia delle misure di sicurezza, supportare il Riesame della Direzione e individuare azioni correttive e opportunità di miglioramento continuo.

Le risorse umane e tecniche sono valutate e adeguate al trattamento dei rischi aziendali. La Direzione approva gli indirizzi e le misure di gestione dei rischi di sicurezza e cybersicurezza, ne supervisiona l'attuazione e assegna ruoli, responsabilità e autorità definiti. Il personale è selezionato secondo procedure interne, è soggetto a obblighi di riservatezza e a processi controllati di ingresso, cambio ruolo e cessazione, ed è formato periodicamente su sicurezza delle informazioni, igiene informatica, phishing, uso sicuro degli strumenti e segnalazione degli incidenti. Ove applicabile la disciplina NIS2, i componenti degli organi di gestione ricevono formazione specifica sui rischi di cybersicurezza e sulle relative responsabilità.

Le risorse tecniche, gli asset informativi e i servizi rilevanti sono censiti, classificati e gestiti lungo il loro ciclo di vita in funzione di criticità, valore e requisiti di sicurezza. Le attività di Vulnerability Assessment, gestione delle configurazioni, patch management e monitoraggio sono pianificate e prioritizzate secondo il rischio.

Le vulnerabilità sono identificate, valutate e trattate con priorità e tempi coerenti con criticità ed esposizione. Acquisizione, sviluppo, configurazione, modifica e manutenzione di sistemi e applicazioni incorporano requisiti di sicurezza fin dalla progettazione, gestione controllata delle modifiche, patching e, ove pertinente, processi di gestione e divulgazione coordinata delle vulnerabilità.

La Business Impact Analysis (BIA) e le procedure di Business Continuity (BC), Disaster Recovery (DR) e gestione delle crisi sono riesaminate periodicamente. Sono definiti, ove applicabili, priorità di ripristino, RTO/RPO, requisiti di backup, copie protette e separate, prove di

ripristino, comunicazioni di emergenza ed esercitazioni periodiche, con registrazione degli esiti e delle azioni di miglioramento.

È mantenuto un processo formalizzato di gestione degli incidenti che comprende rilevazione, registrazione, classificazione, escalation, contenimento, analisi, ripristino, conservazione delle evidenze e riesame post-incidente. Il personale deve segnalare tempestivamente incidenti, eventi sospetti e near miss attraverso i canali definiti.

Ove la disciplina NIS2 sia applicabile, l'escalation interna e la raccolta delle informazioni sono organizzate in modo da consentire le notifiche ad ACN/CSIRT Italia nei termini previsti dalla normativa e dalle specifiche vigenti, inclusi gli eventuali aggiornamenti e la relazione finale.

WIN S.r.l. - Wineuropa.it fornisce sostegno a tutte le parti interessate, interne ed esterne per garantire l'efficacia del sistema nel realizzare le strategie aziendali.

I fornitori e i prestatori di servizi sono selezionati, qualificati e monitorati in funzione del rischio e della criticità dei servizi forniti. I requisiti di sicurezza sono definiti contrattualmente e comprendono, ove pertinenti, riservatezza, protezione dei dati, livelli di servizio e continuità, gestione degli incidenti e relative comunicazioni, controllo dei subfornitori, diritto di verifica o evidenze di assurance, gestione delle modifiche e condizioni di cessazione o migrazione del servizio.

Gli accessi ai sistemi interni ed esterni, fisici e virtuali, sono gestiti secondo i principi di necessità, minimo privilegio e separazione dei compiti. Sono utilizzate identità individuali, procedure di autorizzazione, revisione periodica e revoca tempestiva degli accessi, controlli specifici per gli account privilegiati e autenticazione a più fattori ove appropriata o richiesta, con particolare attenzione agli accessi remoti e ai sistemi critici.

Riservatezza, integrità, disponibilità e, ove pertinente, autenticità delle informazioni sono alla base dell'attività di WIN S.r.l. - Wineuropa.it e dei rapporti con fornitori e collaboratori. Reti,

sistemi e informazioni sono protetti mediante misure tecniche e organizzative commisurate al rischio, quali configurazioni sicure, segmentazione, firewall, EDR/antimalware, IDS/IPS, registrazione e monitoraggio degli eventi, cifratura dei dati e delle comunicazioni ove appropriata, VPN e canali sicuri, backup protetti e autenticazione forte.

Le informazioni sono classificate e trattate secondo il livello di sensibilità e criticità; per ciascuna classe sono definiti requisiti coerenti di accesso, trasmissione, conservazione, backup, condivisione, retention e cancellazione o distruzione sicura dei dati e dei supporti.

Tutti sono chiamati a dare il loro contributo per la prevenzione di fatti che potrebbero in qualche modo alterare la riservatezza, integrità e disponibilità delle informazioni.

Tutti i sistemi interni sono soggetti a controllo lungo l'intero ciclo di vita. Acquisizione, inventario, configurazione sicura, sviluppo, collaudo, messa in esercizio, gestione delle modifiche, monitoraggio, manutenzione, fine vita e dismissione di apparati, software, reti, dati e supporti avvengono in modo documentato e secondo procedure definite; le modifiche rilevanti sono valutate sotto il profilo del rischio e verificate prima del rilascio.

La presente Politica è approvata dalla Direzione, comunicata all'interno dell'organizzazione e resa disponibile alle Parti Interessate ove appropriato. È riesaminata almeno annualmente e ogni qualvolta intervengano cambiamenti significativi del contesto, dei servizi, dell'organizzazione, dei requisiti legali o regolamentari, delle minacce, a seguito di incidenti significativi o di rilevanti risultanze di audit e Riesame della Direzione. Gli aggiornamenti, le approvazioni e le comunicazioni sono documentati; la comprensione e l'applicazione della Politica sono sostenute da attività periodiche di sensibilizzazione e formazione.