ALLEGATO 1 - POLITICA DEL SISTEMA INTEGRATO

ISO 9001 – ISO/IEC 27001 – ISO/IEC 27017 – ISO/IEC 27018

In conformità ai contenuti del Manuale di gestione integrato per la Qualità e la Sicurezza delle Informazioni, il presente documento riassume la Politica aziendale fondata sui seguenti principi:

1. La soddisfazione del Cliente significa rispettare le sue esigenze e le sue aspettative.
2. Garantire:
    - l'eccellenza nell'erogazione dei propri servizi;
    - la massima flessibilità nei confronti del cliente;
    - la professionalità;
    - il rispetto delle esigenze del cliente.
    - il rispetto delle procedure interne per la gestione sicura degli asset e dati aziendali
    - l'impegno al rispetto della normativa applicabile, sia per quanto concerne la qualità del servizio erogato, che per l'assicurazione di più elevati standard di sicurezza delle informazioni;
    - gli obiettivi definiti per i processi principali con monitoraggio semestrale
    - i tre principali obiettivi della sicurezza delle informazioni:
        - la **Disponibilità**: ovvero, assicurare che gli utenti autorizzati abbiano l'accesso alle informazioni e agli asset associati quando necessario;
        - la **Riservatezza**: ovvero, garantire che le informazioni siano accessibili solo dalle persone autorizzate ad averne l'accesso;
        - l'**Integrità**: ovvero, proteggere l'esattezza e la completezza delle informazioni e le modalità di trattamento delle stesse.
3. Valutare il proprio rischio attraverso la definizione della:
    - Reale probabilità che un evento accada
    - Vulnerabilità dell'oggetto dell'analisi, rispetto agli eventi minacciosi
    - Valenza preventiva delle contromisure implementate
    - Possibilità del danno derivante da un potenziale incidente di sicurezza;
    - Valenza mitigativa degli effetti dannosi delle contromisure implementate.
4. Per l'implementazione ed erogazione dei servizi in cloud, ai sensi della ISO/IEC 27017 e della ISO/IEC27018 e del Regolamento (UE) 2016/679, la direzione si impegna ad adottare requisiti di sicurezza e di conformità normativa per garantire anche la protezione dei dati personali degli interessati e che prendano in considerazione i rischi derivanti dal personale interno, la gestione sicura del multi-tenancy (condivisione dell'infrastruttura), l'accesso agli asset in cloud dei clienti da parte del personale del service provider, il controllo degli accessi (in particolare degli amministratori), le comunicazioni ai clienti in occasione di cambiamenti dell'infrastruttura, la sicurezza dei sistemi di virtualizzazione, la protezione e l'accesso dei dati dei clienti in ambiente cloud, la gestione del ciclo di vita degli account cloud dei clienti, la comunicazione dei data breach e linee guida per la condivisione delle informazioni a supporto delle attività nonché la costante sicurezza sull'ubicazione fisica dei dati nei server in cloud. Asystel Italia opera in qualità di Cloud Service Provider nei confronti dei propri clienti per offrire servizi in cloud computing in modalità PaaS, SaaS e IaaS. Per l'erogazione di detti servizi si avvale di propri fornitori nei confronti dei quali assume il ruolo di Cloud Service Customer. Con riferimento ai propri clienti Asystel, ai sensi della ISO/IEC 27018 e in accordo con Regolamento (UE) 2016/679, agisce come Titolare ovvero come Responsabile del Trattamento, dichiarando il rispettivo status e i relativi obblighi che ne discendono nei contratti sottoscritti e nelle nomine a responsabile che Asystel prevede con i propri fornitori per lo svolgimento delle attività di trattamento. A tal fine Asystel pone cura ed attenzione alla corretta identificazione degli interessati dei dati personali che tratta, all'esattezza dei dati personali di cui viene in possesso, alla liceità dei trattamenti che esegue su tali dati, alla ponderata identificazione, valutazione e gestione di tutti i rischi connessi con i diversi trattamenti eseguiti, con eventuale esecuzione di valutazioni di impatto (DPIA), all'adozione di misure tecniche e organizzative adeguate (processi, strumenti e controlli idonei) per garantire, ed essere in grado di dimostrare, che ogni trattamento è effettuato conformemente alla normativa vigente in materia di protezione dei dati personali, all'adozione di criteri e metodi di "privacy by design" e "privacy by default" per la piena conformità ai dettami normativi, all'identificazione delle responsabilità e autorità coinvolte nella gestione dei dati personali trattati anche afferenti alle nomine pertinenti di DPO (Data Protection Officer), Delegati e Autorizzati al trattamento, Amministratori di Sistema, Responsabili del trattamento.
5. La formulazione di politiche e procedure dedicate per la sicurezza dei trattamenti, compatibilmente con i requisiti della ISO/IEC 27001 e ISO/IEC 27018.

6. La sensibilizzazione e la formazione del personale e dei fornitori (quando opportuno) per il sostegno delle attività di prevenzione e gestione nel sistema privacy
7. Adeguati flussi informativi da e verso gli organi sociali, le strutture di controllo e operative per la gestione dei processi di protezione dei dati
8. Il più ampio coinvolgimento di tutto il personale è requisito fondamentale per il continuo miglioramento dei servizi erogati.
9. Le attività previste dal Sistema di gestione integrato sono lo strumento per realizzare efficacemente tale coinvolgimento e concorrere al miglioramento dei servizi.
10. L'Amministratore Delegato, a partire dalle esigenze del Cliente e da quelle del mercato, definisce annualmente gli obiettivi e le risorse per il Sistema integrato.
11. I Fornitori, i clienti e tutte le parti interessate sono componente essenziale della ns società e sono coinvolti nel nostro programma di miglioramento e valutazione dei rischi ed opportunità.
12. La protezione dei dati personali dei clienti e di tutti i soggetti coinvolti nel Sistema di Gestione è elemento costitutivo della sicurezza delle informazioni e pertanto è oggetto di cura e gestione del sistema integrato adottato ed è pertanto intesa come inscindibile dalla politica del sistema.
13. Il successo della ns società richiede il miglioramento professionale e culturale delle singole risorse a tutti i livelli. È pertanto prevista l'individuazione di un preciso e coerente Piano di Formazione volto all'effettiva crescita.

Questa politica viene periodicamente rivista dalla Direzione e aggiornata se necessario, secondo i cambiamenti che hanno effetto sul Sistema di Gestione Integrato per la Qualità e la Sicurezza delle Informazioni che è stato implementato.

Milano, 07 marzo 2023 AD: *Emanuela Verzeni*