ALLEGATO 1 - POLITICA DEL SISTEMA INTEGRATO
ISO 9001 – ISO/IEC 27001 – ISO/IEC 27017 – ISO/IEC 27018

In conformità a quanto previsto dal Manuale di Gestione Integrato per la Qualità e la Sicurezza delle Informazioni, la presente Politica esprime i principi e gli impegni di **Asystel-BDF S.p.A.** nel garantire la qualità dei servizi erogati e la protezione delle informazioni trattate anche in cloud.

Asystel-BDF fonda il proprio Sistema di Gestione Integrato sui seguenti principi:

- La **soddisfazione del cliente**, intesa come capacità di comprendere e rispondere alle sue esigenze e aspettative.
- L'**eccellenza dei servizi** erogati, perseguita attraverso professionalità, competenza e flessibilità operativa.
- Il **rispetto delle procedure aziendali** per la gestione sicura degli asset e dei dati aziendali.
- L'**aderenza alla normativa applicabile**, sia in materia di qualità del servizio che di sicurezza delle informazioni.

La Società si impegna altresì a garantire il conseguimento dei tre obiettivi fondamentali della sicurezza delle informazioni:

- **Disponibilità**: assicurare che gli utenti autorizzati possano accedere alle informazioni e agli asset associati quando necessario.
- **Riservatezza**: garantire che le informazioni siano accessibili solo a persone debitamente autorizzate.
- **Integrità**: proteggere l'esattezza, la completezza e l'affidabilità delle informazioni e dei relativi trattamenti.

Gli obiettivi dei processi principali vengono definiti e monitorati periodicamente per verificarne l'efficacia e favorire il miglioramento continuo.
La gestione dei rischi si basa sulla valutazione di:

- probabilità di accadimento di eventi indesiderati,
- vulnerabilità degli asset rispetto alle minacce,
- efficacia delle contromisure preventive e mitigative adottate,
- potenziale impatto derivante da incidenti di sicurezza.

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
- la costante sicurezza sull'ubicazione fisica dei dati nei server in cloud.

Asystel-BDF 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-BDF, ai sensi della ISO/IEC27018 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-BDF prevede con i propri fornitori per lo svolgimento delle attività di trattamento. A tal fine Asystel-BDF 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.

In coerenza con la norma ISO/IEC 27018, la Società si impegna esplicitamente a proteggere i dati personali dei propri clienti nell'ambito della gestione degli aspetti cloud, assicurando che tali dati siano trattati nel rispetto dei principi di liceità, correttezza, trasparenza e minimizzazione, in conformità con il Regolamento (UE) 2016/679 e con i requisiti specifici della norma stessa. Tale impegno comprende la tutela dei dati in ambienti PaaS, SaaS e IaaS e l'adozione di misure tecniche e organizzative adeguate per garantire la sicurezza, la riservatezza e l'integrità dei dati trattati nei servizi cloud.

La Società riconosce che il successo e l'efficacia del Sistema di Gestione dipendono dal coinvolgimento e dalla consapevolezza del personale. A tal fine, promuove:

- un **piano di formazione coerente** con le responsabilità e i rischi dei diversi ruoli,
- una **cultura della sicurezza informatica** basata su responsabilizzazione, comunicazione e prevenzione,
- la sensibilizzazione di dipendenti e fornitori, quando opportuno, al rispetto delle buone pratiche di sicurezza e privacy.
- Adeguati flussi informativi da e verso gli organi sociali, le strutture di controllo e operative per la gestione dei processi di protezione dei dati

Tutti i dipendenti e collaboratori sono tenuti a comprendere il proprio ruolo nella protezione delle informazioni e dei dati personali, contribuendo attivamente alla prevenzione di incidenti e alla salvaguardia del patrimonio informativo aziendale e dei clienti.

La Direzione riconosce che la sicurezza delle informazioni e la qualità dei servizi rappresentano obiettivi dinamici e in continua evoluzione. Pertanto, la Società si impegna a perseguire un processo di miglioramento continuo del proprio Sistema di Gestione Integrato, volto a incrementare l'efficacia delle misure di sicurezza e dei controlli implementati, migliorare le prestazioni complessive del sistema e riesaminare periodicamente obiettivi, rischi e opportunità in un'ottica di innovazione e adattamento ai mutamenti tecnologici e normativi. La Direzione si impegna altresì a mantenere e migliorare costantemente l'efficacia del Sistema di Gestione Integrato, attraverso:

- la definizione annuale di obiettivi misurabili e risorse adeguate;
- il riesame periodico dei risultati e dei rischi;
- l'identificazione di opportunità di miglioramento tecnologico e organizzativo.

I Fornitori, i clienti e tutte le parti interessate sono componente essenziale di Asystel-BDF e sono coinvolti nel programma di miglioramento e valutazione dei rischi ed opportunità.

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.

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, 14 gennaio 2026 AD: *Emanuela Verzeni*