POLITICA INTEGRATIVA PER LA SICUREZZA DELLE INFORMAZIONI IN AMBITO CLOUD

La Direzione di Odoardo Zecca Srl, attraverso la presente Politica Integrativa, stabilisce e formalizza il proprio impegno inderogabile a garantire la sicurezza delle informazioni e la protezione dei dati nei servizi cloud erogati.

A tal fine, la Direzione dichiara e si impegna ad attuare i seguenti principi:

1. Responsabilità del Management e Protezione dei Dati Personali (PII)

Il Management di Odoardo Zecca Srl si assume la piena e diretta responsabilità nel proteggere i dati personali (PII - Personally Identifiable Information) dei Clienti in rigoroso accordo con la legislazione vigente (Regolamento UE 2016/679 - GDPR). Ci impegniamo a esplicitare formalmente, all'interno di tutti i contratti e DPA stipulati, le esatte responsabilità intercorrenti tra Odoardo Zecca Srl (in veste di PII Processor / Responsabile del trattamento), gli eventuali sub-fornitori (Subcontractor) e il Cliente (Titolare del trattamento). Tali responsabilità sono e saranno sempre delineate in diretta relazione al tipo di servizio cloud contrattualizzato (specificando i confini operativi del nostro modello SaaS e l'utilizzo di risorse IaaS/PaaS di terze parti).

2. Requisiti di base per la progettazione e l'implementazione

Ci impegniamo a garantire che la progettazione e l'implementazione dell'infrastruttura SaaS rispettino nativamente i requisiti di base di sicurezza (*security by design* e *by default*). Adotteremo framework di sviluppo sicuro, eseguiremo analisi delle minacce (*threat modeling*) in fase architetturale e applicheremo configurazioni di hardening standardizzate per ogni componente del servizio cloud.

3. Gestione dei rischi da personale interno autorizzato

Ci impegniamo ad applicare controlli rigorosi per mitigare qualsiasi rischio derivante dal nostro personale interno autorizzato ad accedere ai sistemi cloud. Garantiamo l'applicazione del principio del privilegio minimo, la segregazione dei compiti (*Segregation of Duties*), la sottoscrizione di NDA specifici e il monitoraggio continuo (auditing) delle operazioni eseguite dagli amministratori sui tenant di produzione.

4. Multi-tenancy e isolamento del cliente cloud

Ci impegniamo a mantenere la nostra infrastruttura cloud in regime di multi-tenancy assicurando l'assoluto e inviolabile isolamento logico di ciascun Cliente. Garantiamo che tale segregazione sia applicata e verificata a livello di elaborazione (container), rete (Virtual Private Cloud dedicati) e storage (partizionamento crittografico), al fine di impedire ogni forma di visibilità cross-tenant.

5. Accesso agli asset del cliente da parte del personale del fornitore

Dichiariamo che l'accesso ai dati, ai log e agli asset del Cliente da parte del nostro personale tecnico è severamente vietato. Ci impegniamo a consentire deroghe unicamente se necessarie per il troubleshooting o per l'erogazione di supporto esplicitamente richiesto, subordinando ogni accesso eccezionale a una formale autorizzazione via ticket, al tracciamento inalterabile e all'immediata revoca dei permessi a operazione conclusa.

6. Procedure di controllo degli accessi e autenticazione forte

Ci impegniamo a proteggere tutti gli accessi amministrativi alla nostra infrastruttura cloud e ai moduli SaaS mediante procedure di autenticazione forte.

7. Comunicazioni durante la gestione dei cambiamenti

Assumiamo il formale impegno di comunicare tempestivamente e con congruo preavviso ai Clienti qualsiasi modifica (*Change Management*) all'infrastruttura o al software che possa impattare sulle prestazioni o sulla sicurezza del servizio SaaS, specificando i tempi di intervento e le misure di salvaguardia adottate.

8. Sicurezza della virtualizzazione

Ci impegniamo a sottoporre le nostre piattaforme di virtualizzazione e containerizzazione a policy di sicurezza stringenti. Assicuriamo l'isolamento dei carichi di lavoro, la tempestiva applicazione delle patch di sicurezza sugli hypervisor e il controllo di integrità crittografica delle immagini prima del loro rilascio nell'ambiente di produzione.

9. Accesso e protezione dei dati del cliente

Ci impegniamo a classificare i dati del Cliente come strettamente confidenziali e a proteggerli integralmente durante tutto il loro ciclo di vita. Garantiamo l'utilizzo esclusivo di protocolli sicuri (TLS) per i dati in transito e l'applicazione di algoritmi di cifratura avanzati (es. AES-256) per i dati a riposo e i relativi backup.

10. Gestione del ciclo di vita degli account dei clienti

Dichiariamo di applicare procedure formalizzate e tracciabili per l'intero ciclo di vita degli account dei Clienti, dal provisioning iniziale fino al de-provisioning. Ci impegniamo a sospendere o revocare immediatamente le utenze in caso di cessazione del contratto, procedendo alla cancellazione o restituzione sicura dei dati nel rispetto delle policy di retention concordate.

11. Comunicazione delle violazioni e supporto forense

In caso di incidente di sicurezza o Data Breach, ci impegniamo ad attivare con priorità assoluta la procedura di gestione degli incidenti, informando tempestivamente il Cliente. Assumiamo l'impegno di condividere in modo trasparente e sicuro i log e le evidenze di sistema necessarie per supportare le indagini forensi del Titolare e agevolare i suoi obblighi di notifica previsti dal GDPR.