ALLEGATO TECNICO DI SICUREZZA (ATS) E CONDIZIONI GENERALI
Specifiche operative autoportanti per la fornitura della "Piattaforma SaaS RETIX e MEROPE"

Preambolo di validità contrattuale
Il presente documento, costituisce l'esposizione formale, completa e autoportante delle specifiche tecniche e di sicurezza applicate da Odoardo Zecca Srl agli applicativi gestiti in modalità di erogazione SaaS. L'accettazione del contratto implica l'accettazione integrale e incondizionata delle presenti specifiche da parte del Cliente, Salvo particolari modifiche riportate all'interno del contratto stesso. Nessun ulteriore accordo o matrice esterna è necessario per definire gli obblighi di sicurezza qui riportati.

Art. 1 – Ripartizione delle Responsabilità per la Sicurezza delle Informazioni

Riferimento ISO/IEC 27017: Paragrafo 6.1.1.
Applicazione: Il modello operativo condiviso prevede che Odoardo Zecca Srl abbia la responsabilità esclusiva dell'hardening dell'infrastruttura cloud che ospita i moduli applicativi (es. RetiX, Merope ecc). L'Azienda Cliente (es. Ente Locale, Ente Privato) detiene la responsabilità esclusiva della profilazione RBAC (Role-Based Access Control) dei propri operatori, nonché della liceità dei dati anagrafici immessi.
Tale ripartizione è tecnicamente segregata (tramite l'isolamento logico degli ambienti in Virtual Private Cloud - VPC dedicati per ogni singola Azienda Cliente, garantendo che i software di amministrazione operino in perimetri di rete stagni).
Ai sensi dell'art. 4 del Reg. UE 2016/679, l'Azienda Cliente agisce in veste di Titolare del Trattamento, mentre Odoardo Zecca Srl si configura formalmente come Responsabile esterno del trattamento (ai sensi dell'art. 28 del Regolamento UE 2016/679 - GDPR) per tutte le operazioni di conservazione, elaborazione e protezione dei dati necessarie all'erogazione del servizio SaaS. A tal fine, a formale completamento e disciplina di tale specifico ruolo sul trattamento di dati personali, deve essere obbligatoriamente stipulato tra le parti un apposito Data Processing Agreement (DPA).

Specifiche di Sicurezza e Manleva
L'architettura di accesso ai servizi SaaS prevede un modello di sicurezza a più livelli, finalizzato a garantire l'isolamento del tenant e la cifratura del traffico dati. Il processo si articola nelle seguenti fasi operative:

1. Instaurazione del Canale Sicuro: Il Cliente stabilisce una connessione tramite tunnel VPN (IPsec o equivalente) per l'interconnessione tra la propria rete locale (o endpoint) e il tenant dedicato ospitato presso l'infrastruttura del Fornitore. Tale canale garantisce l'instradamento cifrato del traffico point-to-point o LAN-to-LAN.
2. Autenticazione di Primo Livello: Una volta stabilita la connettività di rete, l'utente procede all'autenticazione per l'accesso all'ambiente operativo. Questo avviene tramite protocollo RDP (Remote Desktop Protocol) o tramite interfaccia web via browser, a seconda della specifica configurazione del servizio. In questa fase è richiesto l'inserimento di un primo set di credenziali (User ID e Password) per l'identificazione della sessione remota.
3. Accesso Applicativo (Second Layer): Ad accesso avvenuto, l'utente deve eseguire l'avvio degli applicativi core del servizio SaaS (gestionali o interfacce di controllo). L'accesso a tali risorse richiede un'ulteriore validazione tramite credenziali applicative distinte, garantendo così un doppio livello di controllo e segregazione degli accessi.

Il Cliente prende atto che l'utilizzo del protocollo RDP (*Remote Desktop Protocol*), seppur veicolato all'interno di un tunnel cifrato IPsec, comporta rischi intrinseci legati alla sicurezza della postazione di lavoro locale (Endpoint). In particolare, Odoardo Zecca non può esercitare alcun controllo sulla corretta manutenzione, protezione antivirus e integrità del sistema operativo del Cliente.
Odoardo Zecca viene sollevato da ogni responsabilità, civile o penale, e il Cliente si impegna a manlevare e tenere indenne Odoardo Zecca da qualsiasi danno, perdita, costo o spesa (inclusi danni da interruzione di servizio o perdita dati) derivanti da:

1. Compromissione dell'Endpoint: Accesso non autorizzato causato da malware, keylogger o vulnerabilità presenti sui dispositivi del Cliente.
2. Gestione Credenziali: Smarrimento, sottrazione o uso improprio delle credenziali di accesso da parte del personale del Cliente.
3. Mancato Hardening Client: Inosservanza da parte del IT Manager del Cliente delle patch di sicurezza e delle configurazioni minime raccomandate per il protocollo RDP.

Art. 2 – Ubicazione Geografica e Giurisdizione dei Dati

Riferimento ISO/IEC 27017: Paragrafi 6.1.3, 18.1.1.
Applicazione: I dati primari e derivati del Cliente sono archiviati fisicamente in Data Center localizzati nel territorio della Repubblica Italiana (o nell'Unione Europea). Qualsiasi controversia legata alla protezione dei dati e all'erogazione del servizio regolata da questo documento è soggetta alla giurisdizione della Repubblica Italiana.

Art. 3 – Classificazione, Etichettatura e Protezione dei Record

Riferimento ISO/IEC 27017: Paragrafi 8.2.2, 18.1.3.
Applicazione: Gli applicativi SaaS erogati da Odoardo Zecca Srl ad oggi non integrano funzionalità native per applicare tag di classificazione ed etichettatura ai record. Odoardo Zecca garantisce la conservazione sicura (backup immutabile) dei record di log tracciati dagli applicativi.

Art. 4 – Gestione degli Accessi e delle Credenziali Utente

Riferimento ISO/IEC 27017: Paragrafi 9.2.1, 9.2.2, 9.2.4.
Applicazione: La registrazione e deregistrazione degli utenti degli applicativi avviene tramite i moduli di amministrazione forniti negli applicativi. Il sistema impone autonomamente password complesse (alfanumeriche, min 8 caratteri), con scadenza trimestrale. Le procedure automatizzate di Odoardo Zecca gestiscono le informazioni segrete di autenticazione applicando algoritmi crittografici irreversibili (hash con salt) ai database delle credenziali.

Art. 5 – Controlli Crittografici

Riferimento ISO/IEC 27017: Paragrafo 10.1.1.
Applicazione: Tutti i dati in transito sono protetti da protocollo TLS 1.2/HTTPS. Per i dati a riposo, Odoardo Zecca implementa la cifratura dei volumi di storage.

Art. 6 – Gestione delle Modifiche al Servizio (Change Management)

Riferimento ISO/IEC 27017: Paragrafo 12.1.2.
Applicazione: Odoardo Zecca fornisce notifica telematica ai referenti di sistema del Cliente in caso di modifiche "Major" (es. aggiornamenti architetturali del software) con un preavviso minimo di 15 giorni. Le finestre di manutenzione ordinarie sono eseguite in fasce orarie notturne predefinite a basso impatto per la mobilità. L'obbligo informativo viene applicato anche in caso di variazioni critiche causate dai provider IaaS/PaaS sottostanti.

Art. 7 – Specifiche delle Funzionalità di Backup

Riferimento ISO/IEC 27017: Paragrafo 12.3.1.
Applicazione: Le specifiche di backup applicate in via standard e irrevocabile a tutti i tenant prevedono: backup completi giornalieri. I backup sono conservati in un'infrastruttura di storage isolata con retention di 30 giorni. Odoardo Zecca o il fornitore Cloud esegue test di ripristino per garantire un Recovery Time Objective (RTO) massimo di 24 ore e un Recovery Point Objective (RPO) massimo di 1 gg.

Art. 8 – Funzionalità di Registrazione Eventi (Logging) e Sincronizzazione Orologi

Riferimento ISO/IEC 27017: Paragrafi 12.4.1, 12.4.4.
Applicazione: L'infrastruttura SaaS di Odoardo Zecca è rigorosamente sincronizzata con server NTP (Network Time Protocol) internazionali basati su UTC. Si prescrive al Cliente di sincronizzare la propria rete locale e i dispositivi hardware sui medesimi standard NTP per garantire la validità forense delle correlazioni temporali tra i sistemi.

Art. 9 – Sviluppo Sicuro e Sicurezza nella Catena di Fornitura

Riferimento ISO/IEC 27017: Paragrafi 14.1.1, 14.2.1, 15.1.2, 15.1.3.
Applicazione: L'infrastruttura applicativa è protetta nativamente da Antivirus ed Antimalware. Il ciclo di sviluppo software (SSDLC) di Odoardo Zecca include obbligatoriamente test di sicurezza (SAST) sul codice sorgente prima di ogni rilascio. Contestualmente, qualora Odoardo Zecca si avvalga di sub-fornitori per l'infrastruttura cloud, impone a questi ultimi il mantenimento continuo delle

certificazioni ISO 27001 e ISO 27017, verificandone annualmente l'aderenza per assicurare che la catena del valore non comprometta i livelli di sicurezza.

Art. 10 – Servizi di Assistenza, Ticketing e Gestione Incidenti (Data Breach)

Riferimento ISO/IEC 27017: Paragrafi 16.1.1, 16.1.2, 16.1.7.

Applicazione: Odoardo Zecca mette a disposizione del Cliente un portale di Ticketing dedicato (Help Desk B2B) per la segnalazione, il tracciamento e la gestione delle problematiche operative e degli eventi relativi alla sicurezza delle informazioni. Il portale è garantito come accessibile e disponibile per l'inserimento dei ticket H24, 7 giorni su 7. La presa in carico e la risoluzione tecnica durante l'orario di ufficio dalle 08:00 alle 17:00, come descritto

In caso di accertata violazione dei dati personali o incidenti di sicurezza (Data Breach) che coinvolgano i tenant del Cliente, Odoardo Zecca si impegna a informare tempestivamente i referenti designati e comunque nei tempi previsti dai DPA stipulati con i clienti. La comunicazione includerà un report dettagliato sull'impatto, le contromisure di mitigazione adottate e i log di sistema necessari per supportare il Cliente nelle proprie indagini forensi e nell'assolvimento degli obblighi di notifica all'Autorità Garante per la Protezione dei Dati Personali (ai sensi dell'art. 33 del GDPR).