ALLEGATO TECNICO DI SICUREZZA E CONTINUITÀ OPERATIVA

Integrazione ai Termini di Servizio (TOS) per la tutela della Supply Chain (Allineamento ISO 27001 e Direttiva NIS2)

1. Premessa e Inquadramento Normativo

Il presente documento definisce le misure tecniche e organizzative (TOMs) adottate da Servereasy S.r.l. per garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi Cloud, IaaS e Data Center erogati. Fermo restando il posizionamento normativo di Servereasy S.r.l. come soggetto "fuori ambito" rispetto agli obblighi di rendicontazione diretta verso l'Agenzia per la Cybersicurezza Nazionale (ACN), l'azienda adotta volontariamente i requisiti di sicurezza previsti dalla Direttiva (UE) 2022/2555 (NIS2) al fine di tutelare la *Supply Chain* dei propri Clienti, operando in rigoroso allineamento con gli standard internazionali ISO/IEC 27001.

2. Sicurezza Fisica e Infrastrutturale

I servizi sono erogati attraverso infrastrutture di proprietà, collocate all'interno del Data Center sito in Settimo Milanese. L'accesso fisico alla struttura è regolamentato e limitato esclusivamente al personale tecnico autorizzato, tracciato e sottoposto a rigidi controlli di sicurezza. L'infrastruttura è dotata di presidi per la continuità elettrica (UPS e gruppi elettrogeni) e di sistemi antincendio regolarmente manutenuti e testati.

3. Sicurezza Logica e Protezione delle Reti

Servereasy S.r.l. applica il paradigma di sicurezza *Zero-Trust*:

- **Segmentazione di Rete:** l'architettura di rete è progettata in modalità *layer-3 to the edge*, garantendo il completo isolamento a livello di rete e l'assenza di domini layer-2 condivisi.
- **Autenticazione e Accessi:** l'accesso amministrativo ai sistemi di gestione e agli *hypervisor* è consentito esclusivamente tramite tunnel VPN cifrato (Wireguard) e subordinato all'utilizzo obbligatorio dell'Autenticazione a Fattore Multiplo (MFA).
- **Gestione Vulnerabilità:** l'azienda esegue programmi ciclici di Vulnerability Assessment (VA) e Penetration Test (PT), applicando rigorose politiche di *patch management* per la risoluzione tempestiva delle vulnerabilità identificate.

4. Resilienza dei Dati, Backup e Anti-Ransomware

Le procedure di salvataggio dei dati sono automatizzate e governate da logiche di *Security by Design*:

- **Piattaforma e Cifratura:** i backup vengono eseguiti regolarmente su architettura dedicata (Proxmox Backup Server) con applicazione di cifratura *Data at Rest*.
- **Protezione Logica Anti-Ransomware:** la difesa contro attacchi di tipo *ransomware* è garantita dalla segregazione dei privilegi, operando in modalità *Append-Only* (senza permessi di cancellazione o sovrascrittura lato client).

- **Integrità e Ripristino:** l’integrità dei dati è assicurata da controlli periodici automatizzati sul file system (ZFS). L’azienda effettua regolarmente test di ripristino (*Restore*) per validare le metriche di RTO e RPO pattuite.

5. Gestione Incidenti ed “Early Warning” (SLA di Sicurezza)

A garanzia della conformità normativa dei propri Clienti (GDPR e NIS2), Servereasy S.r.l. ha implementato un processo strutturato per la gestione delle crisi cibernetiche:

- **Notifica Tempestiva:** in caso di violazione della sicurezza (Data Breach) o di incidente cibernetico con impatto grave sui servizi, l’azienda si impegna a fornire una notifica di *Early Warning* al Cliente entro 24/72 ore dal rilevamento, fornendo i dettagli tecnici necessari per le valutazioni di competenza del Cliente.
- **Incident Response:** l’azienda dispone di un *Crisis Team* interno formato e addestrato tramite simulazioni periodiche (*Tabletop Test*) per la gestione degli attacchi informatici (es. mitigazione DDoS in-house, isolamento *malware*).

6. Qualifica del Personale e Politiche di Sicurezza

Tutto il personale tecnico e amministrativo di Servereasy S.r.l. è vincolato da rigidi Accordi di Non Divulgazione (NDA) e sottoposto a un programma di formazione continua in materia di *Cybersecurity* e *Data Protection*. Le postazioni di lavoro remoto sono protette tramite cifratura integrale dei dischi, obbligo di connessione sicura e divieto tecnico di archiviazione locale dei dati aziendali o dei Clienti.