Rev. 00

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

ISO 27001, ISO 27017 e ISO 27018

1. Introduzione

L'organizzazione **LEVITA SRL** che opera nell'ambito di **erogazione servizi di**

- **IAAS+SAAS**
- **Virtual Private Server (VPS)**
- **Provider di posta elettronica**
- **Servizi di hosting (siti web)**
- **Cloud Backup**
- **Register Domain**

riconosce l'importanza della sicurezza delle informazioni per garantire la riservatezza, l'integrità e la disponibilità dei dati critici. La presente politica è stata sviluppata in conformità con i requisiti delle norme ISO/IEC 27001:2024, ISO/IEC 27017:2021 e ISO/IEC 27018:2020 per stabilire l'impegno dell'organizzazione per proteggere le informazioni e mitigare i rischi associati.

L'azienda ha inoltre deciso di sostenere il proprio impegno PER LA SICUREZZA DELLE INFORMAZIONI creando una integrazione al Sistema di Gestione conforme alla norma UNI EN ISO 27001:2024 e alle sue estensioni ISO/IEC 27017:2021 e ISO/IEC 27018:2020 e richiedendo la certificazione di entrambi.

2. Ambito

Questa politica si applica a tutti i processi, i sistemi e le attività che coinvolgono la gestione delle informazioni all'interno dell'organizzazione, indipendentemente dalla loro forma o supporto. I servizi in cloud vengono erogati garantendo i seguenti standard di sicurezza delle informazioni:

- impiego di **data center** con livello minimo **tier4**.
- creazione di VM indipendenti e isolate per erogare i servizi ai singoli clienti.
- accesso controllato e limitato alle proprie risorse per ogni singolo cliente.
- applicazione di eventuale autenticazione MFA per l'accesso alle risorse in cloud.
- comunicazione via mail ad hoc secondo necessità (es. manutenzioni, incidenti, breach, modifiche rilevanti all'infrastruttura, ecc…) fornendo almeno le seguenti informazioni minime:

- tipologia evento da comunicare
- pianificazione temporale di sviluppo dell'evento
- descrizione tecnica dell'evento e delle infrastrutture coinvolte
- notifica di completamento dell'evento/intervento
- garanzia della totale riservatezza dei dati contenuti nelle VM dei clienti

3. Obiettivi

Gli obiettivi principali della politica per la sicurezza delle informazioni sono:

- Garantire la riservatezza, l'integrità e la disponibilità delle informazioni.
- Identificare e valutare i rischi per la sicurezza delle informazioni e adottare misure appropriate per mitigarli.
- Assicurare il rispetto delle leggi, delle normative e degli obblighi contrattuali relativi alla sicurezza delle informazioni.
- Promuovere la consapevolezza e la formazione del personale per garantire una cultura della sicurezza delle informazioni.
- Monitorare e migliorare continuamente il sistema di gestione della sicurezza delle informazioni per garantire la sua efficacia e rilevanza.
- Compliance al GDPR;
- Utilizzo, per le attività lavorative, dei soli dispositivi portatili messi a disposizione dall'organizzazione secondo gli specifici requisiti di sicurezza definiti nelle procedure di Sicurezza delle Informazioni;

Questi obiettivi verranno controllati, a cura di ADS (Amministratore di sistema), mediante gli indicatori di periodo, i cui valori verranno fissati ogni anno dalla Direzione.

Gli obiettivi sopra specificati costituiscono un costante riferimento per tutto il personale, che deve impegnarsi per il loro ottenimento.

4. Responsabilità

La responsabilità per l'implementazione e il mantenimento del sistema di gestione della sicurezza delle informazioni è assegnata alla Direzione. Il Responsabile della Sicurezza delle Informazioni (RSI) è incaricato di coordinare e supervisionare le attività legate alla sicurezza delle informazioni.

5. Gestione dei Rischi

L'organizzazione adotta un approccio basato sui rischi per identificare, valutare e trattare i rischi per la sicurezza delle informazioni in conformità con i principi delle norme ISO/IEC 27001:2013, ISO/IEC 27017:2015 e ISO/IEC 27018:2019.

6. Accesso e Controllo delle Informazioni

L'accesso alle informazioni è limitato al personale autorizzato in base al principio del "bisogno di sapere". Sono implementati controlli di accesso appropriati per garantire l'identificazione positiva degli utenti e proteggere le informazioni da accessi non autorizzati.

7. Formazione e Consapevolezza

Tutto il personale riceve formazione regolare sulla sicurezza delle informazioni e le sue responsabilità in conformità con i requisiti delle norme ISO/IEC 27001:2024, ISO/IEC 27017:2021 e ISO/IEC 27018:2020.

8. Monitoraggio e Miglioramento Continuo

Il sistema di gestione della sicurezza delle informazioni è soggetto a monitoraggio costante per identificare le inefficienze e le opportunità di miglioramento. Sono effettuati audit interni regolari per valutare la conformità e l'efficacia del sistema.

9. Conformità Legale e Normativa

L'organizzazione si impegna a rispettare tutte le leggi, le normative e gli obblighi contrattuali applicabili in materia di sicurezza delle informazioni, inclusi i requisiti delle norme ISO/IEC 27001:2024, ISO/IEC 27017:2021 e ISO/IEC 27018:2020.

10. Revisione della Politica

Questa politica sarà soggetta a revisione periodica per garantire la sua conformità con i requisiti delle norme ISO/IEC 27001:2024, ISO/IEC 27017:2021 e ISO/IEC 27018:2020 e l'evoluzione del contesto organizzativo e delle minacce alla sicurezza delle informazioni.

Nota: Questa politica è vincolante per tutto il personale e le parti interessate dell'organizzazione e deve essere seguita rigorosamente per garantire la sicurezza delle informazioni in conformità con i requisiti delle norme ISO/IEC 27001:2024, ISO/IEC 27017:2021 e ISO/IEC 27018:2020.

Perugia, 28/06/2024

LEVITA SRL
Michele Busiri Vici