

Sommario

1. Obiettivo del documento	2
2. Ambito	2
3. Dichiarazione di conformità	2
4. Policy	2

1. Obiettivo del documento

Si riportano nel presente documento gli accordi relativi alla Sicurezza delle Informazioni per i servizi contrattualizzati in ambito Cloud e le informazioni dovute dal fornitore Lascaux S.r.l. (nel seguito indicato come "Fornitore".) Lo scopo della policy è definire le procedure associate alla sicurezza in relazione ai sistemi informativi, le reti, i dati, i database e le altre risorse informative basate su cloud di Lascaux S.r.l..

Il presente documento di Policy garantisce la riservatezza, l'integrità e la disponibilità dei dati memorizzati, manipolati e resi accessibili utilizzando i servizi di cloud computing. Stabilisce un quadro di responsabilità e di azioni necessarie per soddisfare i requisiti normativi e linee guida di sicurezza in ambiente cloud.

Ulteriori politiche che regolano altre attività di sicurezza delle informazioni, come l'Informativa Privacy, saranno trattate separatamente.

2. Ambito

Questa Policy si applica a tutti i dati di clienti, utenti dei servizi, dati personali e altri dati gestiti dall'Organizzazione, identificati come particolari dalle Policy di classificazione dei dati di Lascaux Srl. e a tutti i servizi gestiti sul cloud da Lascaux s.r.l.

Tutti i servizi erogati in Cloud che rientrano nelle suddette categorie, sono soggetti ai requisiti specificati nel presente documento. I requisiti si applicano alle nuove installazioni ed alle installazioni esistenti. Ogni utente che interagisce con i servizi in cloud di Lascaux S.r.l. è soggetto alle procedure e direttive presenti nel presente documento di Policy Cloud.

3. Dichiarazione di conformità

Lascaux Srl garantisce ai propri Clienti l'applicazione di una serie di misure idonee alla protezione **di tutti i dati**, tra cui l'adozione, l'applicazione e la certificazione di conformità della/alla norma di sicurezza volontaria

ISO/IEC 27001:2013 "Information technology - Security techniques - Code of practice for information security management" ed il rispetto delle linee guida;

ISO/IEC 27017:2021 "Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services;

ISO/IEC 27018:2020 "Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors".

4. Policy

La riservatezza, l'integrità e la disponibilità di tutte le applicazioni informatiche, dei dati, dei sistemi e delle risorse di rete implementate in un ambiente cloud presso Lascaux Srl sono gestite da un Sistema formale di gestione della sicurezza delle informazioni. Questo Sistema fornisce un metodo controllato e ordinato per richiedere e concedere l'accesso ai sistemi informativi di Lascaux Srl basati sul cloud, per monitorare e analizzare la sicurezza dei sistemi e dei dati basati sul cloud, per affrontare e ridurre le violazioni della sicurezza del cloud e per richiedere, testare, approvare e comunicare le modifiche ai sistemi e alle procedure di sicurezza del cloud a fini di audit e di registrazione.

1. La policy coinvolge tutte le tecnologie, i sistemi, i dati e le reti di Lascaux Srl implementate tramite infrastrutture cloud private. Coinvolge inoltre tutte le risorse IT di Lascaux Srl implementate tramite servizi cloud.
2. Lascaux Srl definisce i processi e le procedure di sicurezza del cloud; protegge ed utilizza software e sistemi specializzati per ridurre la minaccia di violazioni della sicurezza del cloud; verifica regolarmente la sicurezza dei perimetri aziendali e di quelli del fornitore di servizi cloud utilizzando test di vulnerabilità ed altri metodi forensi e documenta tutte le informazioni relative alle procedure ed i controlli del cloud.
3. Lascaux Srl prepara e documenta i piani di sicurezza informatica e di cybersecurity con particolare attenzione

ai servizi cloud; facilita la manutenzione e la revisione di tali piani.

4. Lascaux Srl conduce periodicamente processi di analisi e gestione del rischio informatico relativamente a minacce e vulnerabilità interne ed esterne, applicabile a tutti gli ambienti cloud.
5. Il reparto IT stabilisce una politica per il supporto di dati implementati nei servizi cloud, la loro creazione, conservazione e distruzione.
6. Lascaux Srl stabilisce una politica per l'accesso ai sistemi, alle reti, alle applicazioni e ai file di Lascaux Srl implementati nei servizi cloud, sia in locale che in remoto, comprese le password ed altri controlli di accesso alla sicurezza del cloud.
7. Lascaux Srl assicura prevenzione da ogni malware (virus, spam, phishing, ed altri tentativi di accesso non autorizzati) tramite l'utilizzo di antivirus e risorse di prevenzione e identificazione delle minacce.
8. Lascaux Srl utilizza esclusivamente fornitori di infrastrutture cloud certificati relativamente alle normative di cui al Capitolo 3.
9. Lascaux Srl stabilisce una politica di sicurezza del perimetro di rete per garantire che vengano impediti i tentativi non autorizzati di penetrare nel sistema cloud interno.
10. Lascaux Srl stabilisce e documenta un processo formale per l'identificazione di un possibile incidente di sicurezza interno al cloud (ad esempio, furto di informazioni, social engineering, accesso non autorizzato ai sistemi), la valutazione della violazione, la determinazione della natura e del possibile impatto della violazione, la notifica della violazione alle figure di competenza, la riduzione al minimo dell'impatto della violazione nel più breve tempo possibile e la documentazione delle misure adottate per la gestione dell'incidente.
11. Lascaux Srl eroga periodicamente ai propri dipendenti e collaboratori corsi di aggiornamento e formazione in merito a tematiche di cloud security.
12. Lascaux Srl include nei controlli di sicurezza del cloud anche piani di Business Continuity e Disaster Recovery.
13. Lascaux Srl definisce le metodologie per la gestione ed il reporting di incidenti di sicurezza Cloud.
14. Lascaux Srl garantisce appropriati SLA per l'erogazione dei servizi forniti, al fine di garantire elevate prestazioni e per il monitoraggio del livello di qualità effettivamente erogato.
15. Lascaux Srl protegge i propri sistemi SaaS tramite strumenti di IPS/IDS proattivi al fine di garantire un livello di sicurezza ottimale.
16. I dati particolari in uso presso Lascaux Srl all'interno di qualsiasi ambiente cloud approvato vengono crittografati.
17. Il transito dei dati nell'erogazione dei servizi in cloud viene protetto tramite apposita crittografia.
18. L'accesso a tutti i servizi erogati in cloud da Lascaux Srl è governato da meccanismi di autenticazione e controllo accessi
19. Lascaux prevede procedure di logging, back-up e restore dei dati sui servizi erogati in Cloud
20. Tutte le modifiche proposte alle operazioni di sicurezza del cloud vengono documentate in modo dettagliato.