# POLITICA PER LA SICUREZZA DELLE INFORMAZIONI E DEL CLOUD

| Preparato da | Verificato da | Data | Versione |
| --- | --- | --- | --- |
| RSGSI | Direzione | 03/08/2026 | 00 |
| | | | |
| | | | |

Il Sistema di Gestione per la Sicurezza delle Informazioni è lo strumento con il quale Valyouness intende proteggere la riservatezza, l'integrità e la disponibilità del proprio patrimonio informativo, ivi incluso le informazioni dei clienti gestite.

Il raggiungimento di adeguati livelli di sicurezza nei processi aziendali, consente a Valyouness di mitigare e contrastare perdite e danneggiamenti che possano avere impatto sulle persone, sull'immagine e la reputazione aziendali, sugli aspetti di natura economica e finanziaria, oltre a consentire la conformità al contesto contrattuale e legislativo vigente in materia di protezione delle informazioni e dei dati personali.

In tale ambito, Valyouness declina operativamente tali principi attraverso i seguenti obiettivi:

**a) In merito alla sicurezza delle informazioni:**

- adottare ed implementare principi e best practice riconosciuti per garantire la Sicurezza delle Informazioni e promuovere l'acquisizione di certificazioni di conformità agli standard di riferimento;
- stabilire un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) in conformità alla norma ISO/IEC 27001:2022, per garantire e proteggere le informazioni proprie, dei propri clienti e di tutti i soggetti interessati di cui si gestiscono informazioni di diversa natura, da eventuali minacce, mediante un costante processo di valutazione del rischio;
- estendere il Sistema di Gestione per la Sicurezza delle Informazioni alle attività in Cloud in conformità con le norme ISOI/IEC 27017:2026 e ISO/IEC 27018:2025, avendo cura di garantire la loro costante ottemperanza;
- garantire il corretto accesso alle giuste informazioni quando necessario e prevenire l'accesso non autorizzato, sia da parte di chi opera in Valyouness, sia di chi opera per suo conto;
- individuare ruoli e responsabilità, da assegnarsi al proprio organico, indipendentemente dal livello gerarchico occupato, coinvolgendo anche i soggetti terzi che svolgono incarichi chiave;
- assegnare le risorse necessarie al fine di assicurare l'impiego di misure idonee per gli aspetti riguardanti la sicurezza fisica, logica ed organizzativa;
- promuovere continuamente il Sistema di Gestione per la Sicurezza delle Informazioni, anche mediante un impegno costante degli Organi e dei Soggetti apicali;
- individuare, documentare ed applicare regole che disciplinano le modalità di utilizzo delle informazioni, dei beni e degli strumenti;
- supportare il personale e i collaboratori aziendali con un'adeguata istruzione e formazione per sensibilizzare in materia di sicurezza informatica al fine di minimizzare i rischi;
- predisporre adeguate misure di reazione e gestione a fronte del verificarsi di incidenti che possono compromettere la sicurezza delle informazioni e la normale operatività;
- garantire la continuità della sicurezza delle informazioni in caso di scenario sfavorevole o qualora si concretizzi una minaccia;

- ridurre quanto più possibile malfunzionamenti dei sistemi di sviluppo e produzione causati da diffusioni di malware, software o codice dannoso;
- tenere costantemente sotto controllo la gestione della capacity nell'ambiente di produzione per evitare che un suo eventuale sovraccarico causi il collasso dei sistemi, causando interruzioni lavorative e downtime non pianificati;
- assicurare che venga eseguito il corretto processo di gestione (riciclo o dismissione) di materiale informativo digitale, contenente dati aziendali, al fine di evitare la perdita di dati e informazioni sensibili;
- mantenere l'osservanza delle disposizioni contrattuali, legislative e regolamentari, in particolare sulla protezione delle informazioni;
- garantire la idonea custodia delle informazioni personali di terzi e loro gestione secondo principi di liceità, proporzionalità e pertinenza;
- impegnarsi a svolgere un processo continuo di miglioramento ed evoluzione del Sistema di Gestione per la Sicurezza delle Informazioni, pianificando, eseguendo, verificando e attuando con continuità misure ed accorgimenti atti al contrasto di potenziali eventi che possano compromettere il patrimonio informativo aziendale.

**b) Come Cloud service provider e cloud service customer**

Valyouness si configura come Cloud Service Provider (CSP), dal momento che eroga i servizi per la *"*Gestione della Sicurezza delle Informazioni per l'erogazione di Piani e Servizi di Welfare, Gift Card e Voucher sociali tramite App o Piattaforma Cloud SaaS*"* per i propri clienti.

Valyouness si configura anche come Cloud Service Customer, in quanto utilizza piattaforma SaaS di AWS per erogare i servizi in modalità SaaS ai suoi clienti.

Nell'erogazione dei servizi SaaS, Valyouness:

- ha valutato i requisiti di sicurezza di base applicabile nella progettazione ed implementazione dei servizi cloud;
- Nell'erogazione dei servizi SaaS verso i propri clienti sono valutati tutti i rischi relativi alla sicurezza delle informazioni all'interno del ciclo annuale di valutazione dei rischi rientranti all'interno del sistema di gestione ISO/IEC 27001;
- ha valutato il rischio derivante dall'operato del suo personale interno nella gestione delle informazioni dei clienti elaborate in Cloud;
- ha garantito che il cliente possa accedere solo ai dati di appartenenza e non abbia nessuna possibilità di accedere fisicamente alle macchine ove sono trattenuti i dati. Per eventuali richieste inerenti ai suoi dati può contattare l'Organizzazione attraverso le modalità di comunicazione formalizzate in sede contrattuale;

- ha garantito che il sistema di virtualizzazione sia sicuro, secondo quanto previsto dalle best practice di mercato;
- permette al cliente, secondo specifiche modalità di autenticazione, di accedere ai dati caricati all'interno del servizio erogato in SaaS garantendo la segregazione delle informazioni tra Clienti;
- garantisce un ciclo di vita delle credenziali degli utenti che usufruiscono del servizio SaaS prontamente eliminando eventuali accessi non più necessari (es. per mancata sottoscrizione del contratto);
- garantisce che eventuali data breach che possono verificarsi, coinvolgendo eventualmente dati personali, sono prontamente gestiti e che è definito un protocollo di segnalazione dell'evento all'autorità competenti;
- ha una specifica procedura scritta per la gestione degli incidenti di sicurezza delle informazioni. Il Cliente deve verificare se l'assegnazione delle responsabilità per la gestione degli incidenti di sicurezza delle informazioni è adeguata e deve assicurarsi che soddisfi i propri requisiti; In caso di incidente che coinvolga la perdita di una o più caratteristiche tra Riservatezza, Integrità, Disponibilità, Autenticità riguardanti informazioni personali (Data Protection), è compito della Parte che identifica l'incidente dare immediata informazione all'altra Parte.

**c) Come Pii processor**

- garantisce che eventuali data breach siano prontamente gestiti attraverso un'apposita procedura di segnalazione dell'evento all'autorità competenti;
- ha formalizzato una specifica procedura per la gestione degli incidenti di sicurezza delle informazioni. Il Cliente di Valyouness ha l'obbligo verificare che l'assegnazione delle responsabilità per la gestione degli incidenti di sicurezza delle informazioni sia adeguata e, pertanto, soddisfi i propri requisiti;
- garantisce che il Management concentri tutti i suoi sforzi sulla protezione continua e sulla segregazione dei dati personali dei clienti, trattati attraverso i servizi cloud proprietari, nel pieno rispetto della normativa vigente;
- si assicura che in caso di incidente che comporti la perdita di una o più delle seguenti caratteristiche delle informazioni personali (PII): riservatezza, integrità, disponibilità e autenticità, l'evento venga prontamente notificato alla parte interessata.
- Qualora necessario, e comunque entro un massimo di 48 ore, Valyouness intende decidere congiuntamente quale Parte debba essere responsabile della segnalazione del Data Breach. La comunicazione al Garante della Privacy, come previsto dal Regolamento UE 2016/679 – GDPR, dovrà essere inviata entro 72 ore dalla presa di consapevolezza dell'accaduto.

Il SGSI comprende tutte le politiche e le procedure messe in atto per il raggiungimento degli obiettivi della sicurezza delle informazioni e del cloud.

L'osservanza della presente politica per la sicurezza delle informazioni e del cloud è obbligatoria per tutti i dipendenti, collaboratori, fornitori, appaltatori, partner e parti esterne che gestiscono informazioni di Valyouness o dei suoi clienti. La Direzione di Valyouness è direttamente responsabile dell'attuazione della politica e dell'osservanza della stessa da parte di tutte le parti interessate.

La Direzione condivide i principi e gli obiettivi dell'SGSI e ne sostiene pienamente la realizzazione e il mantenimento, fornendo le risorse necessarie a tale scopo.

Con l'obiettivo della massima trasparenza e collaborazione la presente politica per la sicurezza delle informazioni e del Cloud è comunicata a tutti i dipendenti e resa disponibile a tutte le parti interessate per quanto ritenuto necessario.

La presente politica è soggetta a revisioni su base periodica e/o in caso di cambiamenti significativi riguardanti la sicurezza delle informazioni, al fine di garantirne l'idoneità, l'adeguatezza e l'efficienza.

Reggio Emilia, 03 agosto 2026 La Direzione