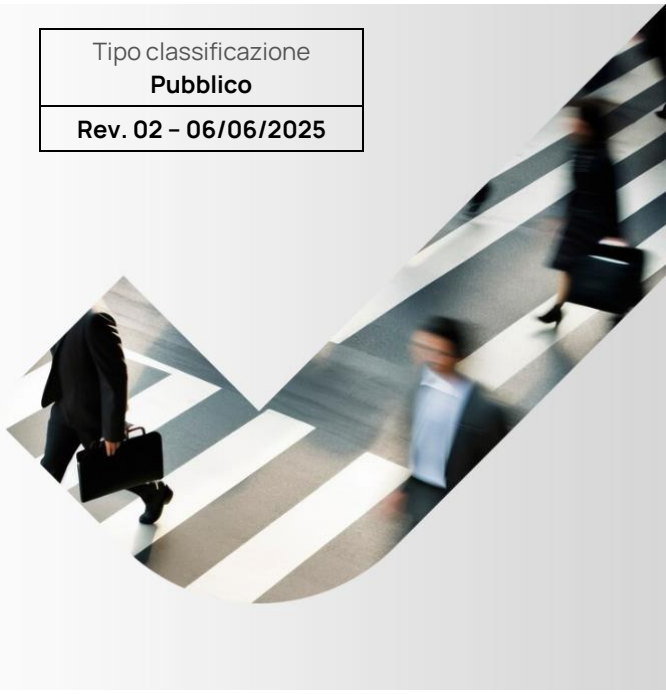
iSimply | Semplicità. Innovazione.

Tipo classificazione
Pubblico
Rev. 02 – 06/06/2025



Politica per la Sicurezza delle Informazioni

La Direzione di **iSimply** ha **definito**, ha **divulgato** e si impegna a mantenere **aggiornata** e attiva a tutti i livelli della propria organizzazione la presente **Politica per la Sicurezza delle Informazioni**, con il fine di **promuovere** e **attuare** efficaci misure di **tutela** e di **protezione** dalle potenziali **minacce**, interne o esterne, intenzionali o accidentali, rivolte alle **informazioni gestite**, **archiviate** e **trasmesse** nell'ambito dei processi aziendali, in conformità con le prescrizioni della norma tecnica **ISO/IEC 27001**.

L'**osservanza** e l'**attuazione** della presente **Politica**, che si realizza concretamente attraverso la **costituzione** e il **mantenimento** di un **Sistema di Gestione per la Sicurezza delle Informazioni** ai sensi della norma tecnica **ISO/IEC 27001**, è pertanto **obbligatoria** per tutto il **personale interno** ed è prevista negli accordi con qualsiasi **soggetto esterno** che, a qualunque titolo, sia coinvolto con il trattamento di informazioni che rientrano nel campo di applicazione di tale **Sistema di Gestione**.

Il **patrimonio informativo** oggetto di tutela è costituito dall'insieme delle **informazioni proprie** o **di terzi**, generate, gestite, archiviate e trasmesse nell'ambito dei processi aziendali attuati in tutte le sedi dell'azienda.

In particolare, tale tutela si realizza attraverso l'attuazione dei seguenti principi:

- **La confidenzialità** delle informazioni: le informazioni devono essere accessibili solo da chi è autorizzato;
- **L'integrità** delle informazioni: le informazioni devono essere protette, in quanto a precisione e completezza, così come i metodi utilizzati per la loro elaborazione;
- **La disponibilità** delle informazioni: gli utenti autorizzati devono poter accedere alle informazioni nel momento in cui lo richiedono.

Per realizzare ciò, l'azienda identifica le proprie **esigenze di sicurezza** tramite una specifica **analisi dei rischi**, che consente di acquisire **consapevolezza** rispetto al **livello di esposizione** a minacce del proprio sistema informativo e permette di **valutare** le potenziali **conseguenze** e i danni che possono derivare dalla mancata applicazione di misure di sicurezza al sistema informativo e quale sia la realistica probabilità di attuazione delle minacce identificate.

A tal fine la Direzione assicura un **supporto** costante e idoneo ai fini della sua **applicazione** e promuove l'introduzione delle eventuali integrazioni e rettifiche necessarie per **adeguarlo ai cambiamenti** che possono influenzare l'approccio dell'Azienda rispetto alla gestione della Qualità, includendo i cambiamenti organizzativi, l'ambiente tecnico, la disponibilità di risorse, le condizioni legali, regolamentari o contrattuali e i risultati dei precedenti riesami.

Il Responsabile del Sistema di Gestione della Qualità ha il compito e la piena autorità di attuare e assicurare il rispetto di quanto sopra enunciato.

I **risultati** di tale valutazione determinano le **azioni** necessarie per **gestire i rischi** individuati e le **misure di sicurezza** più idonee.

I **principi generali** della gestione della sicurezza delle informazioni abbracciano vari aspetti:

1) **E' disponibile un inventario** costantemente aggiornato **degli asset aziendali rilevanti**
2) **Le informazioni sono classificate** in base al loro livello di criticità, in modo da essere gestite con livelli di riservatezza ed integrità coerenti ed appropriati;
3) **Ogni accesso alle informazioni è sottoposto a una procedura d'identificazione e autenticazione**, e le autorizzazioni di accesso alle informazioni sono differenziate in base al ruolo e agli incarichi ricoperti;
4) **Sono definite opportune procedure per l'utilizzo sicuro dei beni aziendali** e delle informazioni;
5) **E' incoraggiata la piena consapevolezza delle problematiche relative alla sicurezza** delle informazioni in tutto il personale (dipendenti e collaboratori) a partire dal momento della selezione e per tutta la durata del rapporto di lavoro.
6) **E' reso disponibile un canale per la pronta segnalazione di eventuali incidenti**, che saranno gestiti secondo specifiche procedure
7) **E' monitorato e impedito l'accesso fisico non autorizzato alle sedi** aziendali
8) **E' assicurata la conformità con i requisiti legali** e con i principi legati alla sicurezza delle informazioni nei contratti con le terze parti.
9) **E' predisposto un piano di continuità** che permetta all'azienda di affrontare efficacemente un evento imprevisto, garantendo il ripristino dei servizi critici in tempi e con modalità che limitino le conseguenze negative sulla missione aziendale.
10) **Gli aspetti di sicurezza sono inclusi in tutte le fasi** di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici;
11) **Si persegue la protezione e la valorizzazione dell'ambiente**, minimizzando l'impatto delle attività aziendali sullo stesso, con particolare attenzione agli effetti sul cambiamento climatico ("climate change").

L'**osservanza** e l'**attuazione** delle **prescrizioni** sopra elencate, compreso l'**obbligo di segnalazione** delle eventuali anomalie e **violazioni** di cui si dovesse venire a conoscenza, sono responsabilità di tutto il **personale** che, a qualsiasi titolo, collabora con l'azienda e di tutti i **soggetti esterni** che intrattengono rapporti e collaborano con l'azienda.

Il Responsabile del **Sistema di Gestione per la Sicurezza delle Informazioni**, nell'ambito del campo di applicazione dello stesso e attraverso norme e procedure appropriate, vigila e opera affinché tale **Sistema** sia costantemente ed efficacemente **attuato**, **aggiornato** e adeguato alla realtà aziendale, anche organizzando opportuni interventi di **formazione** e promuovendo la **consapevolezza** del personale per tutto ciò che concerne la sicurezza delle informazioni.
Chiunque, dipendenti, consulenti e/o collaboratori esterni dell'azienda, in modo intenzionale o riconducibile a negligenza**, disattenda le regole di sicurezza** stabilite e in tal modo provochi un danno all'azienda, potrà essere **perseguito** nelle opportune sedi e nel pieno rispetto dei vincoli di legge e contrattuali.

La Direzione **sostiene** e **promuove** attivamente la sicurezza delle informazioni all'interno dell'azienda tramite un **chiaro indirizzo**, un **impegno** evidente, l'assegnazione di **incarichi** espliciti e il riconoscimento delle **responsabilità** relative alla sicurezza delle informazioni.
La Direzione inoltre **verifica** e **riesamina**, periodicamente o in concomitanza di cambiamenti significativi, l'**adeguatezza** della presente **Politica** e l'**efficacia** e l'**efficienza** del **Sistema di Gestione per la Sicurezza delle Informazioni**, assicurando un supporto costante e idoneo ai fini della sua applicazione e promuovendo l'introduzione delle eventuali **integrazioni** e rettifiche necessarie per **adeguarlo ai cambiamenti** che possono influenzare l'approccio dell'azienda rispetto alla gestione della sicurezza delle informazioni, includendo i **cambiamenti organizzativi**, l'**ambiente tecnico**, la **disponibilità di risorse**, le **condizioni legali**, regolamentari o contrattuali e i **risultati dei precedenti riesami**.
Il risultato di tale riesame include le **decisioni** e le **azioni** relative al **miglioramento** dell'approccio aziendale inerente alla gestione della sicurezza delle informazioni.

La Direzione