# **POLICY SUL SISTEMA DI SICUREZZA DELLE INFORMAZIONI**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | Policy sul sistema di sicurezza delle informazioni | | |
| **Date** | ${psis\_01} | **Version** | 1.0 |

Organizzazione - Titolare del trattamento: ${psis \_02a}

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Firma del rappresentante autorizzato

1. Scopo

La presente Policy sul sistema di sicurezza delle informazioni ("la Policy") regola le misure e le procedure utilizzate per prevenire la perdita o la divulgazione non autorizzata e disciplina l'individuazione e l'eliminazione delle conseguenze in caso di perdita o divulgazione non autorizzata dei dati personali trattati dal titolare del trattamento ${psis \_02b} ("Organizzazione"), nonché delle informazioni ufficiali dell'Organizzazione.

1. Definizioni

Tutte le definizioni contenute nella presente Informativa scritte in maiuscolo (es. Informazioni personali) avranno lo stesso significato di quelle definite in altri atti interni dell'Organizzazione, a meno che non sia espressamente specificato e definito diversamente nella presente Informativa.

I termini a cui si fa riferimento nella presente Politica hanno il seguente significato:

**Dati ufficiali:** documento, ossia qualsiasi documento scritto, riprodotto, disegnato, illustrato, stampato, registrato, fotografato, magnetico, ottico, elettronico o qualsiasi altra registrazione di dati, conoscenze, misure, procedure, argomenti, comunicazioni orali o informazioni, che, in relazione al suo contenuto, ha importanza di riservatezza e integrità per l'Organizzazione, in particolare i segreti aziendali e i dati personali, le informazioni sui contratti stipulati e sulle componenti essenziali del contratto, sulle condizioni di fornitura dei servizi da parte dell'Organizzazione, il know-how dell'Organizzazione, ecc.

**Sistema informativo**: un sistema informatico, di comunicazione o altro sistema elettronico in cui i dati ufficiali sono trattati, conservati o trasmessi in modo da essere accessibili e utilizzabili dalle persone autorizzate, comprendente l'infrastruttura tecnica, l'organizzazione, le persone e le procedure con cui i dati sono trattati, conservati o trasmessi.

**Approccio**: qualsiasi azione che comporti la possibilità di consultare, recuperare, divulgare, modificare o cancellare i dati;

**Misure di sicurezza**: insieme di misure e procedure, a livello tecnico e organizzativo, la cui applicazione consente di raggiungere e mantenere un livello accettabile di protezione della sicurezza del Sistema Informativo.

**Incidente di sicurezza**: un evento che minaccia la riservatezza, l'integrità e la disponibilità dei Dati ufficiali, l'integrità e la sicurezza del Sistema informativo, o che indica un accesso non autorizzato al Sistema informativo.

1. Applicazione del Regolamento

Il presente Regolamento si applica a tutti i dipendenti (Persone Autorizzate) e ai collaboratori esterni dell'Organizzazione che sono autorizzati ad accedere al Sistema Informativo.

Ai collaboratori esterni dell'Organizzazione possono, se necessario, essere riconosciuti i diritti delle Persone autorizzate, fermo restando che le disposizioni della presente Policy si applicano anche nei loro confronti.

La violazione delle disposizioni della presente Policy da parte delle persone autorizzate può comportare la risoluzione straordinaria del contratto di lavoro e, in caso di violazione da parte di collaboratori esterni dell'Organizzazione, la risoluzione del rapporto contrattuale.

1. Diritti e obblighi delle persone autorizzate

Le persone autorizzate sono nominate dal responsabile all'interno dell'Organizzazione e sono individuate in base al luogo di lavoro e ai processi aziendali che svolgono; a tale proposito, l'ambito di autorizzazione all'accesso al Sistema Informativo è determinato in base alle esigenze del luogo di lavoro.

L'ambito dell'autorizzazione di accesso al Sistema Informativo concessa alla persona autorizzata non può superare i poteri conferiti alla persona autorizzata nel regolare processo aziendale.

Le persone autorizzate sono tenute a rispettare le disposizioni della presente Policy al fine di garantire il corretto funzionamento e la sicurezza del Sistema Informativo e di prevenire incidenti di sicurezza.

Le persone autorizzate sono tenute ad adottare tutte le misure di sicurezza prescritte nella presente Policy e altre misure di sicurezza ragionevoli per garantire il corretto funzionamento e la sicurezza del Sistema Informativo e per prevenire o eliminare gli incidenti di sicurezza.

1. Protezione del sistema informativo

**5.1. Controllo e protezione dell'accesso**

La persona responsabile all'interno dell'Organizzazione concede i diritti di accesso al Sistema Informativo alle persone autorizzate in base alle esigenze del loro posto di lavoro, nella misura minima necessaria per lo svolgimento dei compiti lavorativi nell'ambito del regolare processo aziendale.

La persona responsabile all'interno dell'Organizzazione conserva i registri delle approvazioni di accesso e rivede gli stessi registri e poteri a seguito di qualsiasi modifica significativa del sistema e almeno una volta all'anno.

Le persone autorizzate ad accedere al Sistema Informativo sono identificate mediante l'utilizzo di username e password; le persone autorizzate sono responsabili della scelta e della conservazione della riservatezza delle password che utilizzano.

Nella scelta della password, la Persona Autorizzata deve avere cura di utilizzare una password forte e regolarmente modificata (almeno una volta all'anno), che deve contenere almeno 12 caratteri e deve contenere uno o più dei seguenti: lettere maiuscole (ABCDE...), minuscole (abcde...), cifre (0-9), simboli (@#$%{}/\'"; . & & >...), caratteri di punteggiatura (?!).

La Persona autorizzata è tenuta a mantenere segreta la password e a non rivelarla ad altre persone. Eccezionalmente, se esiste una necessità giustificata di accesso a una particolare parte del Sistema Informativo da parte di un'altra persona autorizzata, e tale parte è accessibile esclusivamente tramite la password della persona autorizzata, quest'ultima può rivelare la password a un'altra persona autorizzata. In tal caso, la Persona autorizzata che ha fornito la password è tenuta a sostituirla senza indugio nel più breve tempo possibile.

In caso di forza maggiore o di assenza dal lavoro, la persona autorizzata, con l'eventuale parere della persona responsabile della protezione dei dati personali nell'Organizzazione, che è l'amministratore del sistema, può ispezionare il Sistema Informativo dell'Organizzazione a scopo di approfondimento dei Dati Ufficiali. L'ispezione viene effettuata solo in relazione ai Dati ufficiali e ai dati necessari per l'ispezione (ad esempio, l'accordo con un partner commerciale su prodotti e servizi, prezzi e date concordate) e dopo l'ispezione viene redatto un registro degli accessi.

**5.2. Regole di utilizzo delle apparecchiature**

Le apparecchiature dell'Organizzazione possono essere utilizzate esclusivamente per scopi aziendali e tutte le apparecchiature devono essere registrate da tutti gli utenti delle stesse.

Le apparecchiature dell'Organizzazione non possono essere utilizzate per scopi privati se non dietro espressa autorizzazione dell'Organizzazione.

L'uso delle apparecchiature dell'Organizzazione, ovvero delle apparecchiature personali utilizzate per scopi aziendali, deve essere conforme alla legge, agli atti interni dell'Organizzazione e ai diritti di licenza.

Le apparecchiature dell'Organizzazione devono essere adeguatamente protette (protezione antivirus), in base al particolare tipo di apparecchiatura dell'Organizzazione.

Le persone autorizzate sono responsabili dell'uso professionale, etico e legale delle apparecchiature dell'Organizzazione e delle apparecchiature personali quando vengono utilizzate per scopi aziendali.

Le attrezzature dell'Organizzazione, ovvero le attrezzature personali utilizzate per scopi aziendali, devono essere protette, ove tecnicamente possibile e non richieda uno sforzo sproporzionato, da un'adeguata password complessa o da qualsiasi altro mezzo che impedisca l'accesso diretto alle stesse da parte di terzi diversi dalle persone autorizzate.

Le persone autorizzate sono tenute a cambiare le password di accesso alle apparecchiature dell'Organizzazione, ovvero alle apparecchiature personali utilizzate per scopi aziendali, almeno una volta all'anno.

Le persone autorizzate sono tenute ad adottare tutte le misure di sicurezza necessarie per evitare l'alienazione delle attrezzature aziendali, ovvero delle attrezzature personali utilizzate per scopi aziendali.

Le persone autorizzate non devono destinare le attrezzature dell'Organizzazione all'uso di terzi e, nel caso di fornitura di attrezzature personali utilizzate per scopi aziendali, devono adottare tutte le misure di sicurezza ragionevoli per evitare il verificarsi di un incidente di sicurezza.

## **5.3. Regole di utilizzo delle apparecchiature personali**

L'uso di apparecchiature personali per scopi aziendali comporta un rischio per l'azienda, che si presenta soprattutto come rischio di accesso non autorizzato, furto e perdita di dati.

È consentito collegare i propri dispositivi di archiviazione dati (ad es. dischi esterni) alle apparecchiature dell'Organizzazione allo scopo di eseguire il backup dei dati e di trasmettere i dati nel caso in cui ciò non sia possibile o non sia sufficientemente pratico per operare attraverso il Sistema Informativo. Prima di utilizzare il proprio dispositivo di archiviazione dati, è necessario controllare il dispositivo e il suo contenuto con uno strumento antivirus. Non è consentito collegare e utilizzare dispositivi infettati da virus o altri programmi dannosi. Se il dispositivo di archiviazione dati si trova al di fuori dei locali dell'Organizzazione, i dati ufficiali e personali presenti sul dispositivo devono essere criptati e inoltre protetti da una password di accesso al dispositivo, se quest'ultimo ha questa possibilità. Quando tutti i dati non sono più necessari, devono essere cancellati in modo sicuro.

Non è consentito copiare e archiviare dati interni e riservati sui propri dispositivi senza la preventiva approvazione dell'Organizzazione. Non è consentito copiare e archiviare sui propri dispositivi e supporti di memorizzazione dati contrassegnati come segreto commerciale, anche in forma criptata.

## **5.4. Uso dei sistemi informativi e delle e-mail ufficiali**

Le persone autorizzate devono utilizzare i sistemi informativi ufficiali dell'Organizzazione e le e-mail ufficiali dell'Organizzazione in modo da evitare danni all'Organizzazione e il verificarsi di un incidente di sicurezza.

I contenuti inviati tramite la posta elettronica ufficiale devono essere scritti in modo accurato e misurato al fine di evitare un incidente di sicurezza.

Il servizio di posta elettronica può essere utilizzato solo per comunicazioni ufficiali. È vietato inviare e-mail dall'indirizzo di posta elettronica ufficiale per scopi privati.

I messaggi sul servizio di posta elettronica ufficiale sono considerati documenti ufficiali.

Non è consentito inoltrare automaticamente le e-mail a un altro account utente, ovvero a un altro indirizzo e-mail non appartenente all'Organizzazione, senza l'autorizzazione dell'amministrazione dell'Organizzazione.

Alla cessazione del rapporto di lavoro o di altro tipo di rapporto contrattuale, la Persona autorizzata al supporto informatico dell'Organizzazione deve assicurarsi che l'account utente della Persona autorizzata venga chiuso, in modo tale che l'account utente venga disattivato con l'ultimo giorno e invii un messaggio elettronico automatico ai mittenti a cui possono rivolgersi, e poi dopo 2 mesi gli account utente vengano cancellati.

## **5.5. Accesso a Internet e utilizzo dei servizi Internet**

L'Organizzazione adotta misure di sicurezza adeguate per impedire l'accesso online non autorizzato al Sistema Informativo dell'Organizzazione, in particolare misure di protezione contro virus e altri programmi distruttivi, compresa l'installazione e l'esecuzione di programmi di protezione contro i virus sulle apparecchiature (dispositivi) utilizzate per l'accesso a Internet.

I programmi utilizzati per la protezione dai virus devono essere aggiornati e le persone autorizzate non devono escludere o disattivare tali aggiornamenti e programmi.

Le persone autorizzate sono tenute a evitare attività online che potrebbero compromettere la sicurezza dei loro computer e del Sistema Informativo dell'Organizzazione e, quando utilizzano Internet, possono visitare solo le pagine necessarie per lo svolgimento del lavoro.

**5.6. Misure di protezione aggiuntive**

Al fine di proteggere il Sistema Informativo, l'Organizzazione deve implementare anche le seguenti misure di protezione:

* Misure di protezione per impedire a persone non autorizzate di utilizzare il Sistema Informativo:

${psis\_03}

* + ${psis\_03\_item}

${/psis\_03}

* Misure volte a garantire che i dati contenuti nel Sistema Informativo non possano essere letti, copiati, modificati o rimossi senza un'autorizzazione appropriata durante il processo di trasferimento elettronico, il trasporto o l'archiviazione su supporti di dati, e che vi sia la possibilità di controllare e identificare il destinatario a cui i dati personali devono essere trasferiti attraverso i sistemi di elaborazione dati:

${psis\_04}

* + ${psis\_04\_item}

${/psis\_04}

* Misure per garantire che i dati contenuti nel Sistema Informativo siano protetti da distruzione o perdita accidentale:

${psis\_05}

* + ${psis\_05\_item}

${/psis\_05}

1. Notifica di un incidente di sicurezza

Le persone autorizzate e i contraenti esterni autorizzati dalle persone autorizzate devono informare senza indugio la direzione dell'Organizzazione o una persona autorizzata designata dalla direzione dell'Organizzazione se vengono a conoscenza di un incidente di sicurezza e di una violazione delle disposizioni della presente Policy, o se rilevano carenze nel funzionamento del Sistema informativo, in particolare nelle misure di sicurezza del Sistema informativo.

1. Disposizioni finali

Al termine del contratto di lavoro o del rapporto contrattuale con l'Organizzazione, tutte le persone autorizzate sono tenute a restituire le attrezzature dell'Organizzazione, nonché qualsiasi altro bene loro assegnato in uso. Inoltre, tutte le persone autorizzate sono tenute a consegnare tutta la documentazione e tutte le informazioni di proprietà dell'Organizzazione. Non è consentito copiare e divulgare i dati ufficiali e personali affidati alle persone autorizzate.

La presente Policy entra in vigore otto giorni dopo la data di pubblicazione.

La presente Policy sarà adeguatamente divulgata alle Persone Autorizzate e il periodo di adattamento per la piena applicazione della Policy sarà di un mese dalla data di adozione.