# 1. Introduzione

## 1.1. Obiettivi del documento

Il presente documento costituisce la dichiarazione delle politiche adottate da Si.Gest.A. SRL riguardo la sicurezza delle informazioni.

L'obiettivo principale di Si.Gest.A. SRL è documentare tutte e strategie attraverso le quali l'azienda si propone di tutelare le informazioni documentate presenti a qualunque titolo nel proprio sistema informativo.

Gli obiettivi sono:

• assicurare l'adozione di procedure finalizzate alla progettazione, all'utilizzo e al mantenimento dei livelli di sicurezza delle informazioni;

• assolvere ai requisiti legislativi, siano essi norme o standard di riferimento;

• garantire che le procedure attuate siano diffuse fra le parti interessate.

Questo viene perseguito attenendosi agli standard internazionali di riferimento in materia, alle disposizioni legislative vigenti in materia di sicurezza, privacy, trattamento dei dati.

Le direttive in merito alla tutela dei dati sono contenute nella documentazione interna di Si.Gest.A. SRL, pertanto questo documento riassume in forma di disposizione i requisiti e le relative procedure riguardanti la sicurezza delle informazioni così come espressi nei vari

documeni nel Sistema Qualità di Si.Gest.A. SRL.

## 1.2. Campo di applicazione

La presente disposizione si applica ad ogni Utente assegnatario di beni e risorse informatiche aziendali ovvero utilizzatore di servizi e risorse informative di pertinenza della Società.

La presente disposizione è pubblica, in quanto i principi in essa contenuti riguardano anche aspetti relativi ai servizi erogati da Si.Gest.A. SRL, e pertanto si ritiene opportuno che gli utenti che utilizzano tali servizi siano messi a conoscenza di tutte le azioni e le procedure interne intraprese da Si.Gest.A. SRL a salvaguardia delle informazioni raccolte o conservate dalla Società.

### 1.3. Definizioni e documentazione di riferimento

Per Utente si intende a titolo esemplificativo e non esaustivo, ogni dipendente, collaboratore (interno o esterno), consulente, fornitore e/o terzo che in modo continuativo e non occasionale operi all'interno della struttura aziendale utilizzandone beni e servizi informatici.

Per Società si intende, invece, la società Si.Gest.A. SRL, la quale opererà per mezzo dei soggetti che ne possiedono la rappresentanza.

Ai fini del GDPR s'intende per:

1) «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

2) «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

3) «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

4) «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

5) «pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

6) «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

7) «titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

8) «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

9) «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

10) «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

11) «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

12) «violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

13) «dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

14) «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

15) «dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

16) «stabilimento principale»:

a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che

quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;

b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

17) «rappresentante»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

18) «impresa»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

19) «gruppo imprenditoriale»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

20) «norme vincolanti d'impresa»: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

21) «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

22) «autorità di controllo interessata»: un'autorità di controllo interessata dal trattamento di dati personali in quanto:

a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;
b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure
c) un reclamo è stato proposto a tale autorità di controllo;

23) «trattamento transfrontaliero»:

a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure
b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

24) «obiezione pertinente e motivata»: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

25) «servizio della società dell'informazione»: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio;

26) «organizzazione internazionale»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

## 2. Disposizione sulla sicurezza delle informazioni

Questo documento comprende tutti gli aspetti relativi a come Si.Gest.A. SRL tratta la sicurezza delle informazioni.

Si.Gest.A. SRL gestisce quotidianamente informazioni appartenenti ai propri clienti, e mette in atto tutte le strategie necessarie per proteggerle e salvaguardarle.

La gestione della sicurezza delle informazioni è parte centrale e fondamentale delle attività di Si.Gest.A. SRL.

Al fine di salvaguardarle al meglio, le informazioni devono essere classificate in base ad un livello adeguato che ne definisca il grado di riservatezza, integrità e disponibilità, che viene definito nel capitolo Classificazione delle informazioni.

Il personale con particolare responsabilità rispetto alle informazioni deve assicurarne il livello di classificazione, e trattarle rispetto al livello individuato.

Deve inoltre mettere in atto tutte le procedure definite dall'azienda per assicurarne la sicurezza, e attenersi alle indicazioni definite nel capitolo Procedure relative alla sicurezza delle informazioni.

Le informazioni vengono protette da accessi non autorizzati e mantenute nel tempo anche grazie alla sicurezza fisica delle strutture di Si.Gest.A. SRL.

Si.Gest.A. SRL ha deciso di impostare la sicurezza del proprio sistema informativo assumendo convenzionalmente, nell'analisi dei rischi, il valore più alto per la probabilità che si possa verificare una minaccia di tipo 'fisico', e concentrando gli sforzi sulla minimizzazione dell'impatto che tali minacce possono determinare, ove si verifichino.

In altre parole, a seguito del verificarsi di una minaccia di tipo "fisico", Si.Gest.A. SRL considera accettabile il rischio del danno economico determinato sulle apparecchiature, purché questo non impatti sulla sicurezza delle informazioni ospitate o gestite dalle stesse.

Tutte le procedure sono pertanto finalizzate a questo obiettivo.

## 2.1. Videosorveglianza

Premesso che

- nelle attività di sorveglianza è necessario rispettare il divieto di controllo a distanza dell'attività lavorativa;
- devono essere osservate le garanzie previste in materia di lavoro quando la videosorveglianza è impiegata per esigenze organizzative e dei processi produttivi, ovvero è richiesta per la sicurezza del lavoro (art. 4, Legge n. 300/1970);
- tali garanzie devono essere rispettate sia all'interno degli edifici, sia in altri luoghi di prestazione di lavoro;
- è inammissibile l'installazione di sistemi di video sorveglianza in luoghi riservati esclusivamente ai lavoratori o non destinati all'attività lavorativa (ad es. bagni, spogliatoi, docce, armadietti e luoghi ricreativi);

INFORMA

- che la società utilizza un sistema di videosorveglianza degli accessi a circuito chiuso al solo fine di garantire la sicurezza ed il patrimonio aziendale e prevenire atti illeciti;
- che ai sensi e per gli effetti del D.Lgs. n. 196/2003 e del Regolamento UE 2016/679 "G.D.P.R.", per esigenze di sicurezza sono presenti apparecchiature di video sorveglianza in funzione solamente durante il periodo di attivazione dell'impianto antifurto;
- che le immagini sono registrate e conservate esclusivamente a cura del personale addetto alla sorveglianza e sono cancellate entro 48 ore successive alla rilevazione, salvo eventuali periodi legati a festività o chiusura, nel rispetto del punto 3.4 del provvedimento del Garante per la protezione dei dati personali del 8.4.2010;
- Le immagini sono consultabili solo dal personale incaricato o dall'autorità giudiziaria o di polizia;
- L'impianto di videosorveglianza a circuito chiuso è costituito da n. 8 telecamere individuate nella planimetria che si allega a questa informativa;
- che l'impianto e le apparecchiature esistenti non riprenderanno luoghi riservati esclusivamente ai dipendenti;
- L'impianto registrerà solo le immagini indispensabili ed è costituito da telecamere orientate verso le aree maggiormente esposte a rischi di furto e danneggiamento

(limitando l'angolo delle riprese ed evitando, quando non indispensabili, immagini dettagliate);

- L'eventuale ripresa di dipendenti e/o visitatori avverrà esclusivamente in via incidentale e con criteri di occasionalità;
- All'impianto non potrà essere apportata alcuna modifica e non potrà essere aggiunta alcuna ulteriore apparecchiatura (se non in conformità all'art. 4 della Legge n. 300/1970 e sempre previa relativa comunicazione alla D.T.L.);
- che il trattamento dei dati personali avverrà nel rispetto dei diritti e delle libertà fondamentali dei cittadini e della dignità delle persone con particolare riferimento alla riservatezza, all'identità ed alla protezione dei dati personali come previsto dal citato GDPR;
- Le informazioni raccolte sono utilizzabili a tutti i fini connessi al rapporto di lavoro;
- I lavoratori potranno verificare periodicamente il corretto utilizzo dell'impianto;
- comunicazione e/o diffusione: i dati non saranno diffusi, venduti o scambiati con soggetti terzi, salvo l'utilizzo in caso di reati perpetrati ai danni della società e/o di terzi; In tal caso le immagini saranno messe a disposizione dell'autorità competente;
- natura del consenso: ai sensi dell'art. 24, D.Lgs. n. 196/2003 e del Regolamento UE 2016/679 "G.D.P.R." il consenso dei suddetti dati non è necessario in quanto gli stessi sono raccolti al fine di preservare e tutelare il patrimonio aziendale e di garantire la sicurezza dei luoghi di lavoro.

## 2.2. Sistema di Conservazione

Fra i vari servizi gestiti da Si.Gest.A. SRL è di particolare rilevanza il servizio rivolto all'esercizio del Sistema di Conservazione, nel quale vengono ospitati e gestiti a norma di legge documenti digitali fiscalmente rilevanti. Il servizio è rivolto sia all'interno di Si.Gest.A. SRL, per la conservazione dei documenti contabili e fiscali inerenti l'attività propria, sia ai Clienti.

Per tale servizio Si.Gest.A. SRL ha definito, oltre alle politiche di sicurezza per le informazioni, anche le disposizioni necessarie per preservare nel tempo i dati archiviati nei propri sistemi.

Tutte le informazioni relative ai formati definiti per la conservazione, la verifica sull'integrità dei file, le soluzioni adottate in caso di anomalie, il monitoraggio e il controllo del sistema, sono contenute nella Procedura DIR01 "Gestione della documentazione".

### 2.3. Ruoli e responsabilità

Vengono di seguito riportati i ruoli assunti all'interno di Si.Gest.A. SRL per quanto riguarda la sicurezza delle informazioni.

Amministratori

Pianifica, controlla e supervisiona le attività della Società.

Formula la Politica della Società e i relativi indirizzi strategici, inclusi quelli riguardanti la sicurezza delle informazioni.

Direzione / Rappresentante della Direzione

Definisce e verifica le informazioni documentate da produrre, e garantisce la loro rintracciabilità e conservazione.

Pianifica, coordina e supervisiona le attività aziendali di concerto con l'Amministratore.

Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni (SiGSI)

Ha la responsabilità di tutte le attività inerenti la sicurezza delle informazioni del sistema informativo di produzione.

Responsabile del Servizio di Conservazione

È il soggetto responsabile della creazione e del mantenimento del sistema e del processo di conservazione documentaria.

Definisce e attua le politiche complessive del Sistema di Conservazione, e ne governa la gestione.

### 2.4. Mantenimento del documento

La responsabilità per la produzione, il mantenimento, e la diffusione del seguente documento appartiene al Responsabile del SiGSI di Si.Gest.A. SRL.

Questo documento è stato approvato dalla Direzione di Si.Gest.A. SRL, e la sua diffusione è pubblica, in quanto rivolta sia al personale interno che agli utenti che utilizzano servizi o prodotti Si.Gest.A. SRL. Il documento è pubblicato sul sito di Si.Gest.A. SRL al

seguente link: www.sigesta.it

Il documento viene rivisto annualmente, o in base alle necessità, per esempio nel caso cambiamenti straordinari nella normativa lo richiedano.

Il documento segue le regole descritte nella Procedura DIR01 “Gestione della documentazione”, e riporta nella parte iniziale i dati relativi a autore, data di rilascio, cambiamenti, approvazione da parte della Direzione.

## 3. Regole sulla sicurezza delle informazioni

Tutte le informazioni devono essere classificate secondo un livello adeguato che ne definisca il grado di riservatezza, integrità e disponibilità.

Riservatezza

L’accesso ai dati deve essere limitato in base ai privilegi indicati per gli utenti definiti,

in accordo con il loro livello di classificazione. Le informazioni devono essere protette da eventuali accessi non autorizzati.

Integrità

Le informazioni devono essere complete e precise. Tutti i sistemi, gli asset e le reti

devono funzionare correttamente, secondo specifiche che ne garantiscano la piena operatività.

Disponibilità

Le informazioni devono essere disponibili all'accesso e poter essere distribuite a chi ne detiene i diritti in base al livello di classificazione.

Tutto il personale di Si.Gest.A. SRL interessato nella creazione o nella gestione delle informazioni deve assicurare che le stesse siano classificate, e che vengano trattate in accordo al livello di classificazione scelto.

Tutti gli utenti interessati da questa disposizione devono trattare le informazioni in accordo con il livello di classificazione scelto.

I principi indicati da Si.Gest.A. SRL per garantire riservatezza, integrità e disponibilità delle informazioni sono i seguenti:

- Ogni utente che venga in possesso di informazioni riservate di Si.Gest.A. SRL è considerato responsabile della protezione delle stesse, soprattutto dall'accesso di terzi e dall'uso non autorizzato;
- Tutti gli utenti hanno la responsabilità di proteggere le loro password aziendali e altre credenziali di accesso collegate ad attività aziendali da un uso non autorizzato;
- Tutti gli accessi e l'utilizzo di informazioni riservate di proprietà di Si.Gest.A. SRL devono essere autorizzate da Si.Gest.A. SRL, per gli scopi connessi all'attività aziendale.
- I dipendenti di Si.Gest.A. SRL e chiunque si trovi ad accedere a informazioni riservate di proprietà di Si.Gest.A. SRL dovranno ricevere una adeguata formazione volta all'addestramento alla protezione delle stesse;
- Tutti gli utenti che utilizzano informazioni riservate appartenenti a Si.Gest.A. SRL devono essere univocamente identificati;
- Le informazioni riservate devono essere protette su qualsiasi dispositivo aziendale;
- Le informazioni riservate devono essere protette anche nel caso l'utente le trasferisca su un dispositivo non aziendale. In tal caso il dispositivo dovrà seguire le regole per i dispositivi aziendali (es.: cellulare personale connesso alla email aziendale);

- Tutti i server che memorizzano informazioni riservate appartenenti a Si.Gest.A. SRL devono essere protetti da accessi non autorizzati.
- Tutti i dispositivi aziendali devono essere adeguatamente censiti e devono esserne note le loro ubicazioni fisiche abituali;
- Nel caso si verifichino spostamenti devono essere seguite le regole per il trasporto;
- I software vanno mantenuti aggiornati su tutti i dispositivi, in modo tale da garantire che le versioni correnti siano le più sicure. Le eventuali patch sono approvate dalla Direzione Tecnica, che provvede ad informare i dipendenti tramite i canali di comunicazione concordati (Skype, messenger, whatsapp, telegram, ecc…) che è possibile aggiornare i dispositivi in sicurezza;

Ogni violazione rispetto alle direttive contenute in questa disposizione deve essere riportata e trasmessa a tutti gli utenti interessati.

## 4. Classificazione delle informazioni

In accordo a quanto definito dalla gestione dei documenti di Si.Gest.A. SRL, le informazioni possono essere classificate come:

- Riservate;
- Confidenziali;
- Pubbliche.

Questa classificazione deriva dalla tipologia delle informazioni (fondamentali o di supporto) e dal pubblico che può avere accesso alle suddette informazioni (ristretto, interno, circoscritto o allargato), secondo il seguente schema:

| | Ristretto | Interno | Circoscritto | Allargato |
|---|---|---|---|---|
| Fondamentale | Riservato | Riservato | Confidenziale | Pubblico |
| Di supporto | Riservato | Confidenziale | Confidenziale | Pubblico |

I documenti che veicolano le informazioni sono di conseguenza così classificati:

**Informazioni fondamentali riservate (uso ristretto o interno):**

Dati sensibili che non sono oggetto di divulgazione al di fuori di un ristretto insieme di addetti.

I documenti che contengono questo tipo di informazioni sono classificati come "Riservati".

**Informazioni fondamentali confidenziali (uso circoscritto):**

Dati che non sono oggetto di divulgazione al pubblico. I documenti che contengono questo tipo di informazioni sono classificati come "Confidenziali".

**Informazioni fondamentali non confidenziali (uso pubblico):**

Dati oggetto di divulgazione al pubblico, senza alcun requisito di riservatezza.

I documenti che contengono questo tipo di informazioni sono classificati come "Pubblici".

**Informazioni di supporto riservate (uso interno):**

Dati che non sono oggetto di divulgazione al di fuori di un ristretto insieme di addetti.

I documenti che contengono questo tipo di informazioni sono classificati come "Riservati".

**Informazioni di supporto confidenziali (uso interno o circoscritto):**

Documenti / informazioni specificatamente legate al Sistema ed al suo funzionamento la cui divulgazione a soggetti non autorizzati potrebbe compromettere l'efficacia delle contromisure poste in essere nel Sistema a protezione della disponibilità, integrità e riservatezza delle informazioni. I documenti che contengono questo tipo di informazioni sono classificati come "Confidenziali".

**Informazioni di supporto non confidenziali (uso pubblico):**

Documenti / informazioni specificatamente legate al Sistema ed al suo funzionamento la cui divulgazione non compromette in alcun modo l'efficacia delle procedure poste in essere nel Sistema.

I documenti che contengono questo tipo di informazioni sono classificati come "Pubblici".

Tutte le informazioni derivate da contatti con i clienti, compresi i documenti portati in conservazione e i dati personali delle registrazioni ai servizi, sono considerate informazioni fondamentali, accessibili solo a un pubblico ristretto, e sono pertanto classificate come riservate.

Le informazioni riguardanti gli utenti dei servizi Si.Gest.A. SRL pertanto non sono assolutamente oggetto di divulgazione al di fuori degli addetti al servizio stesso, e sono soggette a cifratura.

### 4.1. Sistema di conservazione

Viene definito per il sistema di conservazione il ruolo di "Produttore", ossia la persona fisica o giuridica responsabile della creazione del Pacchetto di Versamento (PDV) e del suo invio verso il sistema di conservazione.

I produttori dei documenti sono considerati un pubblico ristretto, e le informazioni versate nel sistema come "fondamentali".

Per questo motivo tutti i dati provenienti dai produttori inseriti nel sistema di conservazione sono considerati come "Informazioni riservate", e non sono oggetto di divulgazione al di fuori del rapporto tra i produttori e i responsabili individuati per il sistema di conservazione.

### 4.2. Utilizzo dei supporti magnetici

Tutti i supporti magnetici riutilizzabili (dischetti, cassette, cartucce, chiavette USB, ecc…) contenenti dati sensibili e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.

I supporti magnetici contenenti dati sensibili e giudiziari devono essere custoditi in archivi chiusi a chiave.

# 5. Procedure relative alla sicurezza delle informazioni

Vengono di seguito riportati gli specifici indirizzi operativi e le indicazioni definite da Si.Gest.A. SRL per perseguire le politiche di sicurezza delle informazioni.

## 5.1. Password

Le password sono una componente fondamentale della sicurezza delle informazioni, in quanto servono a proteggere adeguatamente tutti gli account connessi all'utente.

Tuttavia, una password mal costruita e mal protetta può comportare la compromissione della sicurezza delle informazioni.

Sono quindi fornite all'interno di questa disposizione le linee guide per la creazione di una password sicura, e per la sua corretta conservazione.

I dipendenti di Si.Gest.A. SRL sono tenuti a garantire che le informazioni sensibili, siano esse in formato cartaceo o elettronico, siano conservate in modo sicuro, e protette da password efficaci.

### 5.1.1. Creazione della password

Per quanto riguarda la creazione di una password, in ottemperanza a quanto descritto nel Codice della Privacy:

- La password deve essere formata dal almeno 8 caratteri alfanumerici.
- Deve contenere sia lettere maiuscole che minuscole.
- Deve contenere almeno un numero.
- Non deve contenere informazioni personali.
- Non deve contenere informazioni legate al lavoro.
- Non deve contenere modelli riconoscibili.

La selezione della parola chiave dovrebbe essere governata da criteri di casualità.

A titolo di esempio, ecco alcune sequenze che NON vanno utilizzate:

- il nome di login (o codice di identificazione personale) in qualsiasi forma (ad esempio: invertito, in maiuscole, duplicato, ecc.);
- il proprio nome, il nome del coniuge, dei propri figli e relativi acronimi;
- il nome del sistema operativo che si sta usando;
- il numero di telefono;
- la data di nascita;
- altre informazioni facilmente ricavabili dall'indirizzo, o parti del codice fiscale;
- nomi di città, nomi propri;
- la targa automobilistica;
- semplici composizioni quali ad esempio "qwerty";
- caratteri sequenziali ripetuti (ad esempio 1111, aaaa, ecc.);
- cifre in progressivo ordine crescente o decrescente;
- parole di senso compiuto in lingua italiana o in una lingua straniera diffusa;
- informazioni legate al lavoro quali nomi di software, hardware, nomi di prodotti o servizi;
- le ultime quattro password;

Per quanto riguarda la creazione della password per l'accesso ai servizi, all'utente sono indicate, al momento della creazione del profilo utente, le medesime linee guida.

Sono inoltre applicati controlli restrittivi al momento della formazione, per i quali una password sotto gli 8 caratteri, che non contiene almeno un numero e lettere sia maiuscole che minuscole, viene rifiutata.

### 5.1.2. Gestione della password

Non dovrebbe essere necessario scrivere la password, ma nel caso ci sia bisogno di scriverla va conservata o in un file criptato o se annotata su supporto cartaceo in un luogo accessibile solo al proprietario, meglio se in forma camuffata. Il modo migliore per mantenere segreta la password è memorizzarla.

Per quanto riguarda la conservazione della password:

- Non va utilizzata la stessa password di accesso ad account Si.Gest.A. SRL e ad account personali dell'utente.
- Se possibile gli utenti dovrebbero utilizzare diverse password per i diversi accessi aziendali.
- Come criteri generali:
- Se il sistema utilizza parole chiave di default, esse debbono esser cambiate subito; non consentire che i controlli di sicurezza siano governati da parola chiave fornite dal fabbricante o dall'installatore.
- Cambiare la parola chiave ogni volta che si ha il sospetto che essa, per un motivo qualsiasi, sia venuta a conoscenza di terzi (ad esempio, per osservazione indiscreta).
- Non inserire le password in programmi ed altri file dove possono essere rintracciate.
- Non condividerle con alcuno. Se una parola chiave deve essere divulgata o viene comunque a conoscenza di terzi, bisogna cambiarla subito.

### 5.2. Gestione della documentazione

La gestione interna della documentazione di Si.Gest.A. SRL è soggetta ai principi generali enunciati per la sicurezza delle informazioni.

Tutte le informazioni documentate, ossia tutti i documenti i documenti prodotti o ricevuti da Si.Gest.A. SRL nello svolgimento delle sue attività, devono essere classificate e conseguentemente gestite all'interno dell'organizzazione come enunciato nei capitoli precedenti.

#### 5.2.1. Utilizzo del Personal Computer

Il Personal Computer affidato al dipendente è uno **strumento di lavoro**. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata. La stessa password deve essere

attivata per l'accesso alla rete, per lo screen saver e per il collegamento a Internet. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte del responsabile dei sistemi informatici aziendali.

Il custode delle parole chiave riservate**,** per l'espletamento delle sue funzioni, ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica interna ed esterna.

Il custode delle parole chiave riservate potrà accedere ai dati ed agli strumenti informatici esclusivamente per permettere alla stessa azienda, titolare del trattamento, di accedere ai dati trattati da ogni incaricato con le modalità fissate dalla stessa azienda, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività aziendale nei casi in cui si renda indispensabile ed indifferibile l'intervento, ad esempio in caso di prolungata assenza od impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato.

Non è consentito installare autonomamente programmi provenienti dall'esterno salvo previa autorizzazione esplicita del responsabile dei sistemi informatici aziendali, in quanto sussiste il grave pericolo di portare Virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.

Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal responsabile dei sistemi informatici della *Si.Gest.A. SRL*.

L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'azienda a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (D. Lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore) che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.

Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo previa autorizzazione esplicita del responsabile dei sistemi informatici aziendali.

Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In ogni caso lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. In ogni caso deve essere attivato lo screen saver e la relativa password.

Non è consentita l'installazione sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, …), se non con l'autorizzazione espressa del responsabile dei sistemi informatici aziendali.

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il responsabile dei sistemi informatici aziendali nel caso in cui vengano rilevati virus.

### 5.2.2. Schermo e scrivania puliti

"Schermo e scrivania puliti" significa trattare gli spazi di lavoro in modo tale per cui non siano mai visibili informazioni sensibili, anche in maniera accidentale. Al fine di proteggere tutti i dati sensibili e confidenziali Si.Gest.A. SRL indica ai suoi dipendenti quali accorgimenti utilizzare affinché gli spazi di lavoro non rendano visibili informazioni sensibili.

La postazione di lavoro è intesa come desktop, ma anche come scrivania, nel caso siano presenti documenti cartacei, e più in generale qualsiasi luogo nel quale siano contenute informazioni sensibili relative a Si.Gest.A. SRL, siano esse di proprietà dell'azienda, relative ai dipendenti, ai clienti o ai fornitori.

- La zona di lavoro deve essere costantemente presidiata, e resa sicura al termine della giornata di lavoro.
- Le postazioni computer devono essere bloccate o spente quando non utilizzate.
- I dati cartacei devono essere resi inaccessibili a terzi quanto non si è presenti alla postazione.
- Nel caso dei dati, in qualsiasi forma, vengano conservati in luoghi chiusi a chiave, le chiavi non devono mai essere lasciate incustodite.

- Le password non vanno mai scritte su foglietti lasciati accanto alla postazione di lavoro, e non vanno conservate in una posizione accessibile (anche un file sul computer non criptato è considerato accessibile).
- I computer vanno impostati in modo che automaticamente si blocchino e richiedano la password dopo più di cinque minuti di inutilizzo.
- Nel caso il proprio cellulare o altri dispositivi siano connessi ad attività aziendali (es. email) le regole per la postazione si applicano anche a loro.
- Nel caso il cellulare sia connesso ad attività aziendale si richiede che esso sia protetto con un codice PIN di almeno 5 cifre, o lettura dell'impronta digitale, o disegno ad almeno 9 punti. È sconsigliato l'utilizzo del riconoscimento facciale.

### 5.2.3. Documenti cartacei

Si.Gest.A. SRL ha individuato un luogo sicuro ove sono di norma custoditi i documenti contenenti dati personali; come regola generale, tali documenti non devono essere asportati da tale luogo sicuro e, ove ciò avvenga, l'asportazione deve essere ridotta al minimo tempo necessario per effettuare le operazioni di trattamento.

Il trattamento delle informazioni cartacee segue gli stessi principi delle informazioni elettroniche, e la loro protezione è da assicurarsi tramite il presidio dell'informazione (custodia in luogo sicuro) e in modo che il suo trasporto non ne metta a repentaglio la riservatezza, l'integrità e la disponibilità.

Pertanto:

- I documenti cartacei vanno custoditi in un luogo sicuro.
- Per tutto il periodo in cui i documenti sono all'esterno del luogo sicuro, l'incaricato non deve mai perderli di vista, adempiendo ad un preciso obbligo di custodia dei documenti stessi.
- Tutte le informazioni stampate devono essere rimosse dalla stampante non appena prodotte.
- I dispositivi quali stampanti e fotocopiatrici vanno controllati, in modo che non trattengano informazioni (es. alcune stampanti hanno una cache che potrebbe memorizzare i file stampati).

- Una volta terminata la loro funzione i documenti cartacei contenenti informazioni sensibili devono essere triturati, in maniera tale da rendere il loro contenuto illeggibile.

### 5.3. Utilizzo della rete di *Si.Gest.A. SRL*

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi, pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup.

Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.

Il responsabile dei sistemi informatici aziendali può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.

Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.

È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. È buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio il formato pdf o file di contenuto grafico) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata

#### 5.3.1. Uso della rete Internet e dei relativi servizi

Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. È assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.

È fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal responsabile dei sistemi informatici aziendali.

È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dalla Direzione e con il rispetto delle normali procedure di acquisto.

È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

È vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

### 5.3.2. Uso della posta elettronica

La casella di posta, assegnata dall'Azienda all'utente, è uno **strumento di lavoro**. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

È fatto divieto di utilizzare le caselle di posta elettronica aziendale ***nome.cognome@sigesta.it*** per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione.

È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per *Si.Gest.A. SRL* deve essere visionata od autorizzata dalla Direzione, o in ogni modo è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.

La documentazione elettronica che costituisce per l'azienda "know how" aziendale tecnico o commerciale protetto (tutelato in base all'art. 6 bis del r.d. 29.6.1939 n.1127), e che, quindi, viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto a tutela del patrimonio dell'impresa, non può essere comunicata all'esterno senza preventiva autorizzazione della Direzione.

È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per la comunicazione ufficiale è obbligatorio avvalersi degli strumenti tradizionali (fax, posta, PEC, ecc…).

Per la trasmissione di file all'interno di *Si.Gest.A. SRL* è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati.

È obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

È vietato inviare catene telematiche (o di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente all'ing. Alessandro Della Vedova, *responsabile dei sistemi informatici aziendali*. Non si devono in alcun caso attivare gli allegati di tali messaggi.

### 5.4. Privacy

Si.Gest.A. SRL segue la normativa nazionale ed Europea per quanto concerne la protezione della privacy.

La società è organizzata nel modo seguente:

Titolare del trattamento:

esercita il potere decisionale sulle finalità e sulle modalità del trattamento ivi compreso il profilo della sicurezza; questi è responsabile delle scelte in materia di sicurezza dei dati trattati della cui mancata adozione risponde anche penalmente;

Responsabili del trattamento:

sono scelti fra le figure aziendali che forniscono idonea garanzia del pieno rispetto delle disposizioni in materia di protezione dei dati personali, ivi compreso il profilo della sicurezza; i responsabili agiscono in base alle istruzioni specifiche ricevute dal titolare e rispondono della loro ingiustificata inosservanza, e hanno obblighi specifici circa la comunicazione di eventuali problematiche la cui risoluzione comporta l'intervento decisionale del titolare;

Amministratori di Sistema:

sono figure essenziali per la sicurezza delle banche dati e la corretta gestione delle reti telematiche. Sono esperti chiamati a svolgere delicate funzioni che comportano la concreta capacità di accedere a tutti i dati che transitano sulle reti aziendali ed istituzionali. Ad essi è affidato spesso anche il compito di vigilare sulla protezione dei sistemi informatici di un'azienda o di una pubblica amministrazione;

Incaricati:

soggetti che, nominati direttamente dal titolare o dal responsabile, operano sotto la loro diretta autorità nel rispetto delle istruzioni da questi ricevute e condivise.

Il Titolare del trattamento dati è: Si.Gest.A. SRL

La sede legale è sita in: Piazzale G. Mazzini n. 10/1 – 33019 Tricesimo (UD)

Il Responsabile dei sistemi informatici aziendali è: ing. Alessandro Della Vedova

Il Custode delle parole chiave è: ing. Alessandro Della Vedova

Si.Gest.A. SRL fornisce ai propri dipendenti, collaboratori, fornitori o consulenti, istruzioni organizzative e tecniche che consentano l'osservanza degli obblighi di legge relativi alla privacy. Per questi obblighi delinea il quadro di sicurezza adottato per il sistema informativa, e definisce tutte le misure per garantire l'affidabilità delle componenti hardware e software ai fini della tutela dei dati personali trattati.

Inoltre, provvede a informare gli utenti di prodotti e servizi delle misure messe in atto per proteggere e conservare i dati personali attraverso le apposite informative.

### 5.5. Contromisure per attacchi informatici basati su malware/virus

Gli attacchi informatici basati sulla diffusione di malware/virus rappresentano un concreto di rischio per la sicurezza delle informazioni a tutti i livelli dell'infrastruttura, dai server, alle postazioni, ai dispositivi mobili.

La strategia di Si.Gest.A. SRL per la riduzione di questo rischio si basa su una serie di contromisure di natura preventiva, difensiva e di intervento per il contenimento del danno.

Le misure preventive adottate sono:

- Privilegiare l'uso di sistemi operativi progettati per la sicurezza, come GNU/Linux, Apple macOS, Microsoft Windows dalla versione 10 in poi.
- Mantenere aggiornati i sistemi operativi con l'ultimo livello di patch disponibile presso fonti affidabili, ovvero repository software Linux dotati di firma GPG e la distribuzione di patch e aggiornamenti automatici per macOS e Windows.
- Privilegiare l'uso di software open source di cui è possibile verificare la sicurezza e l'affidabilità in prima persona e di concerto con la comunità di sviluppatori e utenti.

Le misure difensive adottate sono:

- Utilizzare e mantenere aggiornata la soluzione antivirus Microsoft Security Essentials sulle postazioni Windows.
- Il controllo periodico sul software del sistema avviene una volta ogni 24 ore.
- Il controllo periodico sull'archivio dei documenti avviene una volta ogni settimana.

Le misure di intervento per il contenimento del danno sono:

Isolare immediatamente i dispositivi su cui venga rilevato malware/virus.

Disattivare le credenziali degli utenti potenzialmente violate a causa della compromissione del dispositivo.

Ripristinare completamente il dispositivo compromesso evitando operazioni di recupero.

L'aggiornamento della soluzione antivirus Microsoft Security Essentials è garantita mediante le impostazioni sul sistema operativo e verificato nel registro del sistema.

| Indice delle revisioni della procedura in edizione 1 | | |
|---|---|---|
| Rev. | Data | Descrizione modifica |
| 0 | 31/07/2018 | Emissione |
| 1 | 06/05/2023 | Aggiornamento indirizzo sede aziendale ed introduzione sistema di gestione della videosorveglianza |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |
| IL RESPONSABILE GARANZIA QUALITA' | | |