**Introduzione**

***Manuale del dipendente***

Il presente Manuale del Dipendente ha valore info-formativo per i dipendenti circa le procedure e norme aziendali e non costituisce integrazione del contratto di lavoro.

***Definizioni***

Nel testo del presente Manuale per "manager" si intenderà il vostro diretto supervisore. Per "noi" o la "Società" si intenderà _____

**Dispositivi personali (Cellulari, smartphone, tablet, etc.)**

L'utilizzo nel locali aziendali di questi strumenti è consentito solo per casi di reale urgenza. Per motivi tecnici e di sicurezza della rete informatica non è consentito collegarsi alla linea WI-FI aziendale con tali strumenti.

**Sicurezza delle informazioni e dati personali-**

***Tutela dei dati personali***

di seguito vengono riportate le istruzioni necessarie al corretto svolgimento dei trattamenti di dati personali e le conseguenti responsabilità:

- il dipendente potrà accedere ai documenti, alle banche dati ed ai sistemi informatici in relazione ai quali gli verranno assegnate credenziali di autenticazione nel rigoroso rispetto dei principi di pertinenza e non eccedenza valutati in relazione alle specifiche mansioni a assegnate.
- i dati dovranno essere:
    a) trattati in modo lecito e secondo correttezza;
    b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini non incompatibili con tali scopi;
    c) esatti e, se necessario, aggiornati;
    d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati.
- il lavoratore potrà effettuare tutte le operazioni necessarie all'espletamento dei compiti assegnati in seno all'Azienda o a garantire la sicurezza dei dati prendendo a riferimento le norme riportate sul presente documento.
- Resta inteso che ogni operazione consistente in:
    - comunicazione dei dati a soggetti diversi da quelli già autorizzati;
    - diffusione di dati;
    - cancellazione o distruzione;

  dovrà essere autorizzata dal responsabile di riferimento.
- il lavoratore è autorizzato a effettuare i trattamenti sopra riportati esclusivamente mediante gli strumenti informatici messi a disposizione dall'Azienda o autorizzati di volta in volta dal Suo responsabile di riferimento.

***NOZIONI generali***

I dati personali: La legge definisce dato personale “qualunque informazione relativa a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale”.

I dati sensibili: Sono i dati personali idonei a rivelare l’origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l’adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Gli "interessati" : Il Codice definisce "interessato", la persona fisica cui si riferiscono i dati personali. Cosa è il trattamento dei dati personali :La legge definisce trattamento dei dati personali “qualunque operazione o complesso di operazioni, . . . , concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati”.

***LE RESPONSABILITÀ’***

Le responsabilità civili, amministrative e penali ricadono in prima istanza sul Titolare del trattamento, sul responsabile nell'ambito della delega ricevuta dal Titolare, sugli incaricati al trattamento che non si attengono alle istruzioni, ai mansionari, alle procedure aziendali ricevute dal proprio responsabile di riferimento e/o nell'ambito delle attività di formazione.

***REGOLE GENERALI E NORME DI COMPORTAMENTO***

Premesso che tutte le informazioni relative alle procedure interne, alle misure di sicurezza adottate, alle caratteristiche tecnico-funzionali delle attrezzature utilizzate per effettuare i trattamenti sono sottoposte alle stesse cautele valide per i dati sensibili nell'espletamento dei suoi incarichi il dipendente dovrà attenersi alle seguenti norme:

- operare nell'assoluto rispetto della riservatezza di qualsiasi dato o informazione ovvero quant'altro venga a conoscenza per effetto delle attività svolte nell’ambito delle proprie competenze attenendosi pedissequamente alle misure di sicurezza, norme di comportamento e regolamenti interni predisposti e periodicamente aggiornati dall'Azienda, che gli verranno comunicati, evitando di:
    - parlarne al di fuori degli uffici destinati alla loro trattazione o in presenza di persone non autorizzate a conoscere i dati oggetto della conversazione;
    - farne oggetto di conversazione con chiunque non sia autorizzato.
- DENUNCIARE O COMUNICARE IMMEDIATAMENTE AL PROPRIO RESPONSABILE DI RIFERIMENTO:
    - l'eventuale smarrimento di documenti o di qualsiasi altro supporto per l'archiviazione (cd-rom, hard disk, pen drive, etc.) contenente i dati personali o informazioni aziendali o riguardanti le attività;
    - inesattezze o alterazioni indebite di qualsiasi tipo di informazioni;
    - qualsiasi compromissione, sospetta o rilevata, della riservatezza, della sicurezza o dell'integrità delle informnazioni aziendali e dati personali.

- COMPORTAMENTO AL TELEFONO – COMUNICAZIONI VERBALI:
  Informazioni confidenziali e Dati personali comuni e sensibili relativi a persone fisiche (dipendenti, utenti, visitatori, collaboratori esterni etc.) non possono essere trattati telefonicamente tranne che nei seguenti casi:

  - l'interlocutore è una persona autorizzata ad accedere ai dati richiesti e non vi sono dubbi circa la sua identità, in particolare, nella gestione dei servizi che comportano il trattamento via telefono di informazioni riservate relative alle merci ed ai trasporti o di dati personali l'interlocutore telefonico potrà essere identificato con la richiesta di dati che lo riguardano già presenti nelle banche dati che solo l'interessato può avere prontamente disponibili.

  - la comunicazione è necessaria per salvaguardare l'incolumità fisica dell'interessato o di terzi,

  Ovviamente durante la conversazione non devono essere presenti persone non autorizzate a conoscere i dati eventualmente comunicati.
  Nel caso sia necessario trattare verbalmente dati personali in situazioni di promiscuità con terzi estranei al trattamento stesso, dovranno essere adottate cautele atte ad evitare l'indebito ascolto della conversazione, ad esempio usando toni di voce adeguati o evitando di ripetere a voce alta dati identificativi degli interessati.

***SICUREZZA DEI DOCUMENTI CARTACEI***

I documenti cartacei:

- Devono essere opportunamente custoditi in modo da evitare che persone non autorizzate li possano visionare. A tal proposito i consegnatari dei documenti:

  - avranno cura di non applicare alle chiavi degli archivi targhette identificatrici,
  - saranno responsabili della loro corretta conservazione.

- Possono essere consultati solamente dal personale che, per ragioni inerenti il proprio incarico, ne ha effettiva necessità.

- Non possono essere dati in consegna ad alcuno se non previa autorizzazione dell'Ufficio originatore o del proprio Responsabile di riferimento.

- Non possono mai essere lasciati incustoditi e devono essere sempre opportunamente riposti prima di lasciare l'area di lavoro.

- Inoltre, al termine della giornata lavorativa tutte le minute, veline, residui di carta in genere, usati per trattare i dati, non possono essere normalmente gettati tra i rifiuti ma devono essere distrutti.

***STRUMENTI ELETTRONICI utilizzo sicurezza e trattamento di dati personali***

I lavoratori sono tenuti ad assicurare che i PC a loro affidati siano al sicuro e trattati con cura. Qualsiasi perdita o danno che risulti derivare da cattivo uso intenzionale o a seguito di negligenza avranno come conseguenza un'azione disciplinare.

Se il lavoratore viene dotato di un PC portatile “laptop” deve assicurare che non venga mai lasciato incustodito.

- qualsiasi device o sistema informatico aziendale (desktop, notebook, tablet, smartphone, risorse di rete, etc.) dato in uso al personale, sia occasionalmente che stabilmente con assegnazione nominativa, è e resta di proprietà dell’istituto e ne è proibita qualsiasi forma di utilizzo per scopi personali, ivi compresa la memorizzazione, anche solo temporanea, di dati/informazione/files non attinenti all’attività lavorativa.

L’Azienda potrà richiedere in qualsiasi momento la restituzione di qualsiasi device dato in uso al personale anche con brevissimo o senza preavviso.

- L'accesso ai dati è permesso utilizzando l’apposito codice identificativo personale (nome utente o user-id) assegnato al dipendente, associato ad una parola chiave (password). Gli incaricati non devono tenere traccia scritta identificabile delle password.

La Password di lavoro:

- è strettamente personale. Non è cedibile a terzi per nessun motivo;
- non deve contenere riferimenti agevolmente riconducibili all’incaricato;
- la sua lunghezza non può essere inferiore agli 8 caratteri;
- deve essere autonomamente modificata al primo utilizzo e, in seguito, almeno ogni 60 giorni. Indipendentemente dall'impostazione dei sistemi, ciascun Incaricato è personalmente responsabile della corretta gestione delle proprie credenziali per l'autenticazione.

**È estremamente importante tutelare la riservatezza della propria password** in considerazione del fatto che, in virtù di specifiche normative riguardanti in particolare la correttezza nella gestione amministrativa, tutte le operazioni di inserimento e modifica dei dati sono loggate centralmente ed associate all’utente che le ha effettuate

- Nell'utilizzo di devices portatili (es.: palmari, computers portatili, etc.) l'assegnatario ha l'obbligo di effettuare un salvataggio dei dati almeno settimanale sull'area di rete a lui assegnata.
  E’ importante ricordare che il Referente delle risorse informatiche è in condizioni di garantire la recuperabilità ed un adeguato livello di sicurezza solo per i file memorizzati su dischi di rete, che sono sottoposti a salvataggio periodico; Ne deriva che è essenziale e obbligatorio salvare sulla rete i file importanti, confidenziali o contenenti dati personali.

- Ogni qual volta gli incaricati devono abbandonare il proprio ufficio o posto di lavoro, anche per breve tempo, devono aver cura di:
  - verificare che persone non autorizzate non possano accedere ai dati personali, eventualmente uscendo dall'ambiente di lavoro in modo che sia necessaria la password per iniziare nuovamente le operazioni;
  - non lasciare supporti per la memorizzazione dei dati (Hard disk removibili, cd, floppy, etc.) incustoditi.

- GESTIONE E CONSERVAZIONE DEI SUPPORTI PER LA MEMORIZZAZIONE DEI DATI - supporti, magnetici e non, contenenti dati personali:
    - vanno custoditi con le stesse modalità valide per i documenti cartacei;
    - non possono essere reimpiegati per altri scopi;
    - in caso di malfunzionamenti, devono essere fisicamente distrutti;

- E' FATTO OBBLIGO DI:
    - impostare lo screensaver con password;
    - denunciare o comunicare immediatamente ai responsabili smarrimenti compromissioni o alterazioni indebite su dati personali;
    - controllare a vista e non abbandonare mai il personale esterno e ospiti presenti nelle aree in cui vengono trattati dati personali ed informazioni riservate e/o relative a merci e trasporti.

- E' TASSATIVAMENTE VIETATO:
    - eseguire qualunque attività installativa o manutentiva sui sistemi elaborazione dati, periferiche comprese, senza autorizzazione del Titolare;
    - l'impianto di qualsiasi opera, software, sistema o servizio accessorio agli apparati e relative periferiche, senza l'autorizzazione del Titolare;
    - limitare in alcun modo l'accesso da parte del Titolare o di suoi incaricati alle postazioni di lavoro;
    - creare nuove banche dati senza l'autorizzazione del Titolare;
    - l'utilizzo sui sistemi aziendali di supporti esterni per l'archiviazione dei dati senza l'esplicita autorizzazione del Titolare.

***Utilizzo della casella di posta elettronica aziendale***

- La casella postale e la rete sono di proprietà dell'Azienda e sono resi disponibili esclusivamente per ragioni di lavoro.

- Non sono previste ipotesi di utilizzo della casella postale a fini personali. Purtuttavia non è possibile escludere a priori una sia pur improbabile ed incidentale presenza di informazioni non attinenti all'attività lavorativa contenute in comunicazioni ricevute dall'esterno, che devono essere immediatamente cancellate. In riferimento a tali informazioni si fa comunque presente che il sistema (server e pc locale) per default ne tiene traccia ed effettua una copia di backup, accessibile per questioni tecniche dal system manager, che ha istruzione di cancellare, previo avviso all'interessato, tutti i dati non attinenti alle attività lavorative ogni qual volta li rilevi, salvo che non costituiscano prova di illeciti perpetrati dal personale che devono essere obbligatoriamente segnalati alle Autorità competenti.

- Comunicazioni (inviate o ricevute) non più necessarie o pertinenti alle attività aziendali devono essere cancellate, con particolare attenzione a quelle contenenti dati personali in modo da evitare una loro conservazione o trattamento eccedenti.

- Per prevenire utilizzi non corretti delle caselle di posta elettronica a piè di pagina di ogni comunicazione inviata verso l'esterno sarà riportato un avviso che, ovviamente, non è consentito cancellare.

- Dovranno essere evitate e-mail oltraggiose e offensive e si dovranno usare tutte le cautele necessarie al fine di scongiurare l'intercettazione della corrispondenza riservata.

- È espressamente vietato l'utilizzo di posta elettronica per la partecipazione a dibattiti, forum, mailinglist e chat, salvo diversa ed esplicita autorizzazione.

- In caso di assenza dal lavoro, la Società potrà accedere alla casella di posta elettronica assegnata al lavoratore per garantire continuità ed efficienza nell'attività lavorativa. Inoltre la manutenzione periodica della rete potrebbe comportare l'esigenza di accesso alle caselle di posta elettronica.

- In quanto strumento di lavoro, la casella di posta elettronica è utilizzata dalla Società per inviare/trattare informazioni anche confidenziali destinate solo a ristretti gruppi di incaricati, è pertanto proibito abilitare altro personale o terze persone all'apertura della propria casella di posta elettronica senza autorizzazione del proprio responsabile di riferimento.

- è categoricamente proibito l'utilizzo di sistemi di interconnessione diversi da quelli autorizzati ed installati dal Referente delle risorse informatiche;

- Se ricevete un allegato che considerate sospetto, ogni dipendente è tenuto ad avvertire immediatamente il proprio responsabile. Il dipendente non deve aprire nessun allegato sospetto.

***Servizio INTERNET***

- Anche il servizio Internet è disponibile esclusivamente per esigenze di lavoro e, conseguentemente, l'azienda non è responsabile per eventuali diversi utilizzi che restano comunque vietati.

- L'accesso al servizio, salvo diverse e documentate autorizzazioni, deve avvenire esclusivamente con le modalità stabilite dall'Azienda. Collegamenti diversi saranno contestati agli interessati.

- In relazione ad un razionale utilizzo di Internet, l'azienda comunica che potranno essere "visitati" solo i siti collegati agli scopi aziendali.

- Non potranno indicativamente essere effettuate operazioni di trading on line, remote banking, shopping virtuale o scarico di software gratuiti a meno che non vi sia una preventiva autorizzazione in tal senso.

- I lavoratori non potranno registrare siti non legati all'attività lavorativa, finalizzati per esempio alla partecipazione a chat, forum, bacheche elettroniche, neppure utilizzando pseudonimi.

- I collegamenti ad Internet e lo svolgimento di tutte le attività tramite le apparecchiature informatiche dovranno durare il minor tempo possibile tenuto conto della mansione affidata.

Anche in questo caso è importante far presente che i sistemi tengono traccia dei siti visitati e delle operazioni effettuate su internet associabili, con particolari procedure, all'utente che le ha compiute.

Tale traccia è accessibile per questioni tecniche al system manager, che ha istruzione:

- di segnalare tutti gli elementi che creano danno all'Azienda o pregiudizio per la sicurezza dei sistemi e, conseguentemente, per i dati su di essi gestiti;

- di cancellare tutti i dati non attinenti alle attività lavorative ogni qual volta li rilevi, salvo che non costituiscano prova di illeciti perpetrati dal personale che devono essere obbligatoriamente segnalati alle Autorità competenti.

In ogni caso la Società periodicamente provvederà, richiamate le garanzie della "privacy" previste dal Regolamento UE 679/2016, anche ad un controllo quantitativo dell'utilizzo della rete, per verificarne un uso equilibrato e coerente con l'attività aziendale.

***Utilizzo di devices aziendali (notebook, tablet, telefoni, fax e fotocopiatrici aziendali***

- Il telefono aziendale affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non sono quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali è consentito solo nel caso di comprovata necessità ed urgenza.

- Qualora venisse assegnato un cellulare aziendale all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Al cellulare aziendale si applicano le medesime regole sopra previste per l'utilizzo del telefono aziendale: in particolare è vietato l'utilizzo del telefono cellulare messo a disposizione per inviare SMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa.

- Si ricorda che i moderni cellulari, così come i tablet, offrono funzionalità simili a quelle di un pc portatile (memorizzazione dati, ricezione mail, etc.) spesso aggiunte alla possibilità di archiviazione ed invio di immagini (sia foto che filmati). A tal proposito si fa presente:

    - l'obbligo di impostare il cellulare in modo che sia necessario il PIN per accedere alla memoria interna ed alla possibilità di effettuare telefonate; ovviamente il PIN dovrà essere gestito con le stesse norme precedentemente descritte per le password. Nell'utilizzo di sistemi più evoluti, quali smartphone, valgono tutti gli obblighi previsti per i PC portatili;
    - il divieto di utilizzare in modo improprio i sistemi di registrazione video e audio offerti dall'apparato;
    - il divieto di memorizzare in via permanente, sul cellulare messo a disposizione, SMS o MMS ricevuti di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa, prestando particolare attenzione a procedere alla loro cancellazione in caso di restituzione dell'apparato e tenendo presente che, in caso di avaria, tale operazione potrebbe non essere effettuabile. Inoltre l'Azienda potrebbe richiedere in qualsiasi momento la restituzione del device, anche con brevissimo o senza preavviso.Non potranno essere, invece, cancellati SMS o MMS correlati all'attività lavorativa contenenti informazioni che non siano state già acquisiti dall'Azienda o necessarie a garantire continuità operativa.

- È vietato l'utilizzo dei fax aziendali per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte del Titolare.

- È vietato l'utilizzo delle fotocopiatrici aziendali per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Titolare.

Il nostro piano di sicurezza informatica prevede il licenziamento e l'avvio di procedimenti penali nei confronti dell'utente che abbia volutamente danneggiato i sistemi o le informazioni ed i dati trattati

**Misure di sicurezza**

***Controllo accessi e sicurezza***

L'esigenza di disciplinare l'accesso del personale alla/e sede/i e ad alcune aree/uffici risponde alla duplice necessità di security e di rispondenza alle leggi dello Stato, è estremamente importate l'assoluto rispetto delle norme di seguito descritte:

- Ai soli fini della sicurezza e controllo accessi, fatta salva la regolamentazione degli straordinari/permessi/ etc., di norma il personale dipendente può accedere agli uffici nei normali orari lavorativi. La permanenza all'interno degli uffici oltre l'orario consentito deve essere autorizzata dal Responsabile competente o dal referente per ragioni di security. L'accesso e permanenza negli uffici il Sabato e nei giorni festivi deve essere autorizzato dal Responsabile competente (Direzione della Sede). =

- **PER NESSUN MOTIVO** gli accessi alle sedi ed alle aree ad accesso controllato (porte e finestre o qualsiasi altra potenziale via di accesso) possono essere lasciati aperti ed incustoditi; a tal proposito è necessario sincerarsi ogni volta dell'effettiva chiusura del varco (che i meccanismi di chiusura siano effettivamente azionati e non solo, ad esempio, "accostati")

- All'interno delle sedi possono essere presenti aree ad accesso controllato debitamente segnalate da specifici avvisi, L'accesso a tali aree è consentito solo alle persone autorizzate dal Referente security della sede o da persone da quest'ultimo delegate. È fatto specifico divieto di accedere a tali Aree se non per motivi di servizio. **Le aree magazzino in cui vengono movimentate, gestite e stoccate le merci sono comunque considerate aree ad accesso controllato.**

***Personale esterno e visitatori:***

- **NON POSSONO MUOVERSI LIBERAMENTE ALL'INTERNO DELLE SEDI ma devono essere sempre accompagnati dal dipendente ospitante, che è responsabile del loro controllo.**

- salvo diversi accordi o particolari esigenze, debitamente comunicate e ratificate, non possono trattenersi all'interno della sede al di fuori del normale orario lavorativo. E' compito del dipendente ospitante far rispettare tale indicazione o segnalare con debito anticipo diverse esigenze al Referente security della sede;

- **È obbligatorio/necessario segnalare immediatamente al proprio responsabile di riferimento ed al Referente security** della sede qualsiasi elemento possa compromettere i livelli di sicurezza della sede; in particolare:
  - la presenza di persone non autorizzate;
  - il danneggiamento di sistemi di chiusura o apparati di sicurezza;
  - accessi indebitamente lasciati aperti.

***NORME DI COMPORTAMENTO E SICUREZZA per il personale che si trattiene oltre il normale orario lavorativo***

Il personale autorizzato a trattenersi oltre il normale orario lavorativo:

- deve SEMPRE portare al seguito il *Documento di riconoscimento aziendale* ed un documento di identità valido per consentire al personale addetto ai presidi di Sicurezza e Vigilanza un'immediata identificazione;

- non potrà spostarsi per nessun motivo dall'area/ufficio in cui deve operare;

- per le sedi con aree uffici ed aree magazzino, prima di spostarsi dall'area in cui deve operare dovrà, su istruzione del *Referente security* o del *Delegato security* competente, avvertire telefonicamente il personale da questi indicato e/o la centrale operativa dell'Istituto di Vigilanza dai quali potrebbe ricevere istruzioni particolari (*es.: attendere qualche minuto o aspettare di essere accompagnato*.)

L'obbligo di avviso telefonico sussiste in ogni caso anche per l'uscita dalla sede al termine dei lavori.

Le suesposte norme hanno lo scopo di:

- garantire l'efficacia dei sistemi di sicurezza;
- evitare situazioni di rischio che potrebbero venire a crearsi per il personale presente nella sede in orari meno presidiati;
- garantire interventi mirati e veloci nelle situazioni di pericolo (*es.: in caso di incendio o malori la guardia può agire con velocità avendo certezza circa la posizione dei dipendenti all'interno dell'Azienda*).

Il personale addetto al servizio di Vigilanza ha istruzione di verificare il materiale portato eventualmente fuori dalla sede, è quindi preferibile che chi si trattiene fuori orario eviti di portare al seguito borse o valigette.

***Art. 4 Statuto dei Lavoratori. Controlli a distanza su apparecchi elettronici utilizzati per rendere la prestazione di lavoro (personal computer, tablet, cellulare, ecc..).***

Per gli altri strumenti elettronici dati in uso all'incaricato, l'Azienda potrà effettuare dei controlli sul loro corretto utilizzo e sul rispetto delle norme aziendali, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale. Le modalità d'uso di tali strumenti elettronici (personal computer, tablet, cellulare, ecc.) sono dettagliatamente descritte nei paragrafi precedenti. Quanto alle modalità di particolari controlli sui personal computer si precisa che gli stessi verranno effettuati con cadenza almeno mensile dall'azienda ed in particolare dal Responsabile IT mediante procedura informatica.

Le informazioni raccolte a seguito di tali controlli potranno essere utilizzate a tutti i fini connessi al rapporto di lavoro, inclusa la possibilità di avviare procedimenti disciplinari sulla base degli esiti dei controlli effettuati.