SOLUTIONS
IT & SOFTWARE ENGINEERING

P.le Lombardia, 10 – 28100 Novara (NO)
P.I., C.F. 02443620030

DISCIPLINARE INFORMATICO AZIENDALE

Redatto in conformità alla normativa europea ed italiana sul trattamento dei dati personali

Ed. 01/2020

P.le Lombardia, 10 – 28100 Novara (NO)
P.I., C.F. 02443620030

Sommario

P.le Lombardia, 10 – 28100 Novara (NO)
P.I., C.F. 02443620030

1. INTRODUZIONE E OBIETTIVI DELLA PROCEDURA

1.1. PRESENTAZIONE AZIENDALE E FINALITÀ DISCIPLINARE

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete internet dai Personal Computer, espone la Società e gli utenti (dipendenti e collaboratori della stessa) a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (sul diritto d'autore e sulla privacy, fra tutte), creando evidenti problemi alla sicurezza e all'immagine dell'Azienda stessa.

Scopo generale del presente documento è illustrare le misure tecniche e organizzative pianificate ed implementate dalla Società al fine di garantire:

- la sicurezza dei dati e delle informazioni, ossia del patrimonio informativo, posseduto e/o gestito dalla Società;
- la protezione dei dati personali trattati dalla Società, con particolare attenzione agli aspetti di riservatezza, integrità e disponibilità:
- il trattamento dei soli dati personali necessari per ogni finalità di trattamento perseguita;
- la compliance alle normative vigenti, nonché alle policy e alle procedure definite internamente dalla Società.

Tra gli obiettivi perseguiti dal presente disciplinare troviamo quello di fornire agli addetti autorizzati le istruzioni necessarie per garantire il rispetto della protezione dei dati personali nella progettazione dei processi aziendali.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza, correttezza e della liceità, fattori che normalmente si adottano nell'ambito dei rapporti di lavoro, la presente procedura mira ad accrescere la consapevolezza del personale sui temi della sicurezza e sulla protezione dei dati, evitando che comportamenti inconsapevoli o irresponsabili possano esporre la Società a vulnerabilità e minacce, in grado di intaccare la sicurezza e l'integrità di dati, informazioni e sistemi.

Le regole definite dal presente documento garantiscono la sicurezza dei dati e dei sistemi nel rispetto e a integrazione:

- delle disposizioni di cui agli artt. 2104 e 2105 codice civile;
- delle disposizioni dei CCNL;
- del Regolamento UE 2016/679 (di seguito "GDPR") e della normativa nazionale vigente in materia di protezione dei dati personali (di seguito Normativa Privacy);
- degli standard internazionali e best practice di settore applicabili;
- delle procedure e regolamenti adottati in azienda;
- delle istruzioni fornite ed indicate al personale coinvolto nelle attività di trattamento di dati personali.

1.2. AMBITO DI APPLICAZIONE

Il presente documento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'azienda, qualsiasi sia il rapporto contrattuale con la stessa, che, in ragione delle mansioni e/o delle attività assegnate e del lavoro e/o della collaborazione da svolgersi:

- abbiano in dotazione un personal computer aziendale, un cellulare o altro dispositivo con connessione a Internet
- abbiano accesso a una casella di posta elettronica aziendale;
- svolgano qualsivoglia attività sui dati e sulle informazioni in possesso e/o gestite dalla Società, con riferimento anche alle attività di trattamento sui dati personali.

Il presente documento traccia il profilo delle vulnerabilità più diffuse mirando a soddisfare tutte le misure di sicurezza organizzative, fisiche e logiche, in ottemperanza ai requisiti normativi, alle policy e procedure interne alla Società e alle best practice di settore applicabili.

Le aree che rappresentano le misure di sicurezza apprestate dalla Società, in qualità di Titolare, a tutela dei dati, si possono raggruppare in misure riguardanti la:

- **sicurezza fisica**: i mezzi e gli strumenti necessari per proteggere persone, cose e ambienti dai rischi (evitare accessi fisici non autorizzati, manutenzione e sicurezza delle apparecchiature hardware contro manomissione e/o furti, ecc.);
- **sicurezza logica**: protezione dei dati attraverso misure di sicurezza di carattere tecnologico (autenticazione, controllo accessi, cifratura, firma digitale, ecc.);
- **sicurezza organizzativa**: regole e procedure finalizzate a disciplinare gli aspetti organizzativi del processo di sicurezza fisica e logica (prescrizioni riguardanti la definizione dei ruoli, distribuzione dei compiti e delle responsabilità, procedure di aggiornamento dei software, procedure di backup etc).

1.3. ENTRATA IN VIGORE

Con l'entrata in vigore del disciplinare tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, si intendono abrogate e sostituite dal presente documento.

Copia del disciplinare verrà pubblicato nella intranet aziendale e consegnato agli utenti in fase di assunzione o inizio del rapporto di collaborazione.

2. DEFINIZIONI

Dato personale: qualsiasi informazione (es. nome) concernente una persona fisica identificata o identificabile anche indirettamente, oppure informazioni (es. codice fiscale, impronta digitale, traffico telefonico, immagine, voce) riguardanti una persona la cui identità può comunque essere accertata mediante informazioni supplementari.

Riservatezza: Principio tale per cui l'informazione deve essere accessibile solo a chi è autorizzato a conoscerla, e che le informazioni devono essere protette sia durante la trasmissione che durante la memorizzazione.

Integrità: Principio tale per cui le informazioni devono essere trattate in modo che siano difese da manomissioni e modifiche non autorizzate. Proprietà del dato di essere corretto e valido. L'integrità implica la completezza (presenza dell'informazione nella sua totalità), l'accuratezza (informazione priva di errori) e validità dell'informazione (informazione derivante da fonti valide e autorizzate).

Disponibilità: Principio tale per cui le informazioni siano raggiungibili ed utilizzabili quando richiesto da soggetti autorizzati, nei tempi, nei luoghi e nelle modalità adeguate alle necessità operative.

Utente: Soggetto che utilizza sistemi d'elaborazione per ottenere o trattare dati e per scambiare informazioni. Nel contesto della presente procedura, per utente deve intendersi ogni dipendente e/o collaboratore in possesso di specifiche credenziali di autenticazione.

Amministratore di Sistema: Soggetto incaricato della gestione e della manutenzione di un sistema di elaborazione dati o di sue componenti.

Autenticazione: La procedura di verifica dell'identità di un utente da parte di un sistema o servizio.

Autorizzazione: La procedura che verifica se un soggetto interno o esterno ha il diritto di compiere una determinata azione.

Incaricato al trattamento / personale addetto autorizzato: Soggetto/utente, dipendente o collaboratore, che ha accesso ai dati personali e che svolge attività di trattamento sugli stessi secondo specifiche istruzioni formalmente impartite dalla Società, in qualità di Titolare del trattamento, e su autorità della stessa.

Soggetto interessato: Persona fisica identificata o identificabile, a cui fanno riferimento i dati personali raccolti/trattati dalla Società. Ad esempio, a seconda dei contesti, soggetto interessato può essere il dipendente, il cliente finale, il fornitore, etc.
Sono esclusi dalla definizione di soggetto interessato le persone giuridiche.

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. NORME COMPORTAMENTALI E ISTRUZIONI OPERATIVE PER GLI UTENTI AUTORIZZATI AL TRATTAMENTO

Sono di seguito riportate una serie di istruzioni e norme comportamentali che ogni utente, formalmente autorizzato dalla Società, deve rispettare per garantire la sicurezza dei dati personali e delle informazioni aziendali in possesso, in gestione e/o sottoposte ad attività di trattamento attraverso l'utilizzo di strumenti informatici da parte della Società.

1.4. CLASSIFICAZIONE DELLE INFORMAZIONI

Sono previste le seguenti classificazioni dei dati/documenti aziendali:

- **riservato:** informazioni gestionali rilevanti, accessibili solo alla Direzione o a soggetti direttamente autorizzati dalla stessa;

- **confidenziale:** informazioni gestionali rilevanti accessibili alla Direzione e ai Responsabili degli uffici; su specifica autorizzazione della Direzione l'accesso può essere consentito ai diretti dipendenti o collaboratori.
- **interno:** informazioni necessarie per lo svolgimento della normale operatività, ovvero informazioni condivisibili con soggetti esterni per attività svolte in favore della Società;
- **pubblico:** informazioni completamente esenti da vincoli di riservatezza e quindi accessibili anche da persone esterne alla Società.

3.1. AUTENTICAZIONE E QUALIFICAZIONE DELLE UTENZE

Le credenziali di accesso - codice di identificazione personale (userid) ed una parola chiave segreta (password) - richieste per l'utilizzo dei servizi informatici non possono essere ceduti a terzi, neppure temporaneamente.

Qualsiasi azione svolta a seguito del processo di autentificazione è attribuita, in termini di responsabilità, all'utente titolare del codice userid, salvo illecito utilizzo da parte di terzi; pertanto:

- la password va conservata con la massima riservatezza e diligenza;
- la postazione di lavoro non deve essere lasciata incustodita o facilmente accessibile.

3.2. GESTIONE DELLE PASSWORD

Le password dovranno essere create secondo criteri che ne garantiscano la sicurezza.

In particolare, le parole chiavi dovranno rispettare le seguenti caratteristiche:

- essere composte da almeno 8 caratteri;
- essere composte da lettere e numeri;
- essere composte da caratteri maiuscoli e minuscoli;
- utilizzare anche caratteri di speciali, come ( ) ! ? • ",; $ %
- non contenere riferimenti agevolmente riconducibili all'utente;
- essere differenti dalle precedenti 3 utilizzate

Le password devono essere modificate al primo utilizzo e, successivamente, almeno ogni novanta giorni.

Nel caso si sospetti che la password abbia perso la segretezza, dovrà essere immediatamente sostituita;

Si raccomanda di non utilizzare la stessa password per sistemi di autenticazione interni all'Azienda e per sistemi di autenticazione esterni non legati all'attività aziendale.

Ove ad un incaricato vengano attribuiti diversi profili di autorizzazione, non deve essere usata la stessa password .

Tutte le password che sono state generate da un incaricato devono essere trattate come informazioni strettamente riservate.

Le password non devono mai essere scritte su documenti cartacei accessibili o archiviate in linea sui sistemi aziendali (server o postazioni di lavoro).

3.3. GESTIONE ED USO DELLE DOTAZIONI AZIENDALI

Qualsiasi dotazione fornita all'utente prevede, da parte dello stesso, impegno alla custodia con la "diligenza del buon padre di famiglia".

3.3.1. FURTI E GUASTI DI APPARATI

Stante la vigenza di quanto sopraindicato, in caso di furto, il dipendente/collaboratore è tenuto a sporgere denuncia all'autorità di competenza e presentarne copia alla Società.

Nella denuncia dovrà essere riportato il modello ed il numero di serie della macchina.

P.le Lombardia, 10 – 28100 Novara (NO)
P.I., C.F. 02443620030

3.3.2. CLEAN DESK POLICY

Gli addetti autorizzati, nello svolgimento delle operazioni del trattamento, controllano e custodiscono con cura e diligenza gli atti e i documenti contenenti dati personali in modo che ad essi non accedano persone prive di autorizzazione, conservandoli negli appositi archivi al termine delle operazioni.

3.3.3. POSTAZIONE DI LAVORO FISSA

La postazione di lavoro, quale strumento a fini esclusivi di lavoro, è affidata al dipendente/collaboratore, che è responsabile dell'utilizzo delle dotazioni informatiche a lui assegnate (PC, stampante, ecc.).

Ogni utilizzo non inerente all'attività lavorativa non è consentito poiché può contribuire ad innescare disservizi, costi di manutenzione e minacce alla sicurezza.

3.3.4. SOFTWARE

È vietato l'uso di programmi diversi da quelli autorizzati, né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione può esporre la Società a gravi responsabilità civili.

Si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore, che impone la presenza nel sistema di software regolarmente licenziato o comunque “open source” e quindi non protetto da detta normativa, vengono sanzionate anche penalmente.

3.3.5. BLOCCO DEL PC

Il PC deve essere bloccato (attivando lo screen saver e la necessità di inserire la password per sbloccarlo) in caso di allontanamento dalla postazione di lavoro e deve essere spento ogni sera, prima di lasciare gli uffici, fatti salvi i PC che, per ragioni di servizio, devono essere raggiungibili in modo controllato da remoto.

3.3.6. FILE DI PROVENIENZA ESTERNA

Tutti i file di provenienza esterna (ricevuti tramite posta elettronica, navigazione Internet o presenti su dispositivi USB collegati direttamente alle postazioni di lavoro) devono essere preventivamente sottoposti a controlli antivirus.

3.3.7. POSTAZIONE DI LAVORO PORTATILE (NOTEBOOK, TABLET)

L'utente è responsabile del PC portatile assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai PC portatili si applicano le regole di utilizzo previste dalla procedura per la postazione di lavoro fissa di cui ai precedenti articoli.

Per ridurre i rischi nell'uso di tali dispositivi sarà cura dell'utente assicurarsi che il dispositivo sia aggiornato, che siano quindi installate le patch di sicurezza del sistema operativo e dei prodotti software utilizzati e siano abilitati i software di protezione (antivirus ecc.)

I PC portatili utilizzati all'esterno, in caso di allontanamento, dovranno essere anch'essi bloccati (attivando lo screen saver e la necessità di inserire la password per sbloccarlo) ed inoltre dovranno essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

Al fine di garantire la sicurezza dei sistemi e delle informazioni potranno essere attivate password di accesso controllato di basso livello (es. Bios) e/o la crittografia del disco fisso.

3.4. GESTIONE DEGLI ACCESSI ALLA RETE INTERNET E AI RELATIVI SERVIZI

Gli accessi alla rete, ai servizi e alle risorse informatiche aziendali sono gestiti mediante i sistemi di autenticazione, autorizzazione e registrazione degli accessi e delle operazioni effettuate.

L'accesso da remoto alla rete aziendale deve avvenire esclusivamente tramite canali di connessione (vpn) o programmi di teleassistenza forniti dalla Società; è quindi vietata l'installazione e l'utilizzo di qualsiasi software di controllo remoto non autorizzato.

L'accesso e l'utilizzo di internet, quale strumento a fini esclusivi di lavoro, è parte integrante delle postazioni di lavoro.

È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.

In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare internet per:

- l'upload o il download di software, nonché l'utilizzo di documenti provenienti da siti web, se non strettamente attinenti all'attività lavorativa (filmati e musica) e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà venire contattato l'Amministratore di Sistema);
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- 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) se non espressamente autorizzati.

Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, la Società rende nota la possibilità di adottare sistemi di blocco o filtri automatici che prevengabo determinate operazioni quali l'upload, il download o l'accesso a determinati siti internet.

È espressamente vietato:

- accedere ai servizi informatici aziendali e/o alle banche dati aziendali non possedendo le credenziali di accesso o mediante l'utilizzo delle credenziali di colleghi autorizzati;
- introdursi abusivamente in un sistema informatico o telematico protetto da misure di sicurezza contro la volontà del titolare del diritto all'accesso anche al fine di acquisire informazioni riservate;

3.5. SERVIZI DI POSTA ELETTRONICA

Le caselle di posta elettronica interna individuali (nome.cognome@dominio.ext) e/o di gruppo (ufficio@dominio.ext) assegnate ai dipendenti e collaboratori dovranno essere utilizzate esclusivamente per ragioni inerenti all'attività lavorativa.

Ogni utente è responsabile del corretto utilizzo.

L'utente può accedere alla sua casella di posta elettronica da tutti gli strumenti che sono stati abilitati (Desktop, Laptop, Tablet, Telefono Mobile, Webmail).

I messaggi inviati o ricevuti dall'utente sono raccolti sul server di posta elettronica aziendale, in cui rimangono conservati in base allo spazio di memoria disponibile per la casella assegnata, secondo le prassi aziendali. Tali messaggi sono archiviati su sistemi di archiviazione aziendale.

Le informazioni contenute nei messaggi di posta elettronica sono da considerarsi riservate e confidenziali.

Il loro utilizzo è consentito esclusivamente ai destinatari in indirizzo e ne è vietata la diffusione in qualunque modo eseguita, salvo che ne sia data espressa autorizzazione da parte del mittente.

È fatto divieto di utilizzare le caselle di posta elettronica aziendali per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica aziendale per:

- trasmettere a soggetti esterni alla Società informazioni riservate o comunque documenti aziendali, se non nel caso in cui ciò sia necessario in ragione delle mansioni svolte, per l'adempimento di un obbligo di legge o di contratto di cui sia parte la Società o al fine di difendere un diritto della Società;
- inviare messaggi aventi contenuto lesivo per la reputazione dell'azienda e che gettino discredito sulla medesima o

P.le Lombardia, 10 – 28100 Novara (NO)
P.I., C.F. 02443620030

il compimento di qualsiasi atto o fatto illecito attraverso l'utilizzo della casella aziendale che possano far attribuire alla Società ed a chi la rappresenta una responsabilità penale, civile od amministrativa;
- l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es.mp3) non legati all'attività lavorativa;
- l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum mailing list;
- la partecipazione a catene telematiche (comunemente dette “di Sant’Antonio”). Se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente all’Amministratore di sistema. Non si dovrà in alcun caso procedere all’apertura degli allegati a tali messaggi.

In caso di assenza prolungata, la Società potrà attivare la funzione di risposta automatica che inviti il mittente a prendere contatto con altre risorse aziendali.

Qualora si debba conoscere il contenuto dei messaggi di posta elettronica delle caselle aziendali, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all’attività lavorativa, si procederà secondo quanto previsto dal presente documento.

3.6. UTILIZZO DISPOSITIVI MOBILI

Per "Dispositivo mobile" è da intendersi il telefono cellulare, il tablet, lo smartphone e ogni altro dispositivo che consenta la gestione di comunicazioni telefoniche, audio, video e di applicativi software "in mobilità".

I dispositivi mobile aziendali non possono essere ceduti né fatti utilizzare a terzi.

In merito all'uso dei device mobili, quali strumenti di lavoro, si precisa che è proibito, senza alcuna eccezione, modificare la configurazione dei dispositivi mobili e/o installare applicazioni sospette o non regolarmente licenziate, manualmente o da uno store di applicazioni (Apple Store, Google Play, ...).

Non è consentito l'uso di qualsiasi dispositivo esterno collegabile al dispositivo mobile, se non quelli aziendali o quelli espressamente autorizzati.

L'utente, ove possibile, deve mantenere aggiornato il sistema operativo e le app del dispositivo mobile.

L'utente non può forzare direttamente e/o indirettamente né installare sul dispositivo mobile sistemi e/o software che consentano di modificarne le funzionalità, di alterarne le caratteristiche o di "prendere il controllo" del sistema operativo (ad es.: jailbreak, root, etc).

I dispositivi mobile devono avere abilitato il codice di blocco e/o il PIN d'accesso e/o la Password personalizzata, secondo le linee guida generali precedentemente Illustrate. Tale codice d'accesso dev'essere impostato al massimo del numero di caratteri consentito dal sistema operativo dello strumento e l'eventuale password utilizzata non deve facilmente richiamare né date di nascita né altri riferimenti anagrafici. Si consiglia l'uso di password alfanumeriche composte anche di lettere maiuscole e simboli, sempre se ammessi dal sistema operativo del mobile in dotazione.

Se il dispositivo mobile consente l'attivazione dei servizi di Tethering ovvero consente la configurazione dell'apparato come gateway per offrire accesso alla Rete ad altri dispositivi che ne sono sprovvisti, questo tipo di possibilità va usata solo per periodi limitati ed in assenza di ogni altra soluzione di connettività (UMTS, Wi-Fi, Rete Ethernet, etc.). Il servizio va immediatamente disattivato al termine dell'utilizzo e va protetto da password almeno alfanumeriche.

Il Bluetooth ed ogni altro protocollo che consenta l'associazione di dispositivi diversi dallo strumento mobile, dev'essere abilitato per l'accoppiamento ai soli strumenti aziendali in dotazione. Inoltre, può essere usato, in particolare, per l'attivazione dell'auricolare personale e/o del kit “viva voce” dell'auto. Il Bluetooth non va mai lasciato inutilmente attivo e le password d'associazione non devono mai essere quelle di default previste per il dispositivo.

È fatto espresso divieto d'utilizzare un qualsiasi dispositivo mobile aziendale durante la guida. L'uso in auto è consentito solo mediante kit "viva voce" e/o con auricolare.

L'eventuale connessione Wi-Fi va abilitata sul dispositivo mobile solo ed esclusivamente ai fini d'accesso alla rete aziendale e/o di altre reti protette e non deve essere mai lasciata inutilmente attiva.

Per quanto attiene ai principi che disciplinano l'utilizzo della connettività internet e della posta elettronica attraverso dispositivi mobili, valgono le regole definite nei paragrafi dedicati.

P.le Lombardia, 10 – 28100 Novara (NO)
P.I., C.F. 02443620030

3.7. UTILIZZO DELLE RISORSE CONDIVISE

Le risorse condivise sono aree di condivisione di informazioni esclusivamente professionali.

Sulle unità di rete vengono svolte regolari attività di controllo, amministrazione e backup da parte dell'amministratore del Sistema.

Per l'accesso alla rete e ai dati è necessaria l'autentificazione dell'Utente.

È richiesta agli utenti, per quanto di loro competenza, la periodica (almeno ogni tre mesi) pulizia degli archivi, con cancellazione dei file obsoleti, duplicati o non più utili.

3.8. PROTEZIONE ANTIVIRUS

La società provvede all'installazione sulle postazioni di lavoro assegnate (sia fissa che portatile) al dipendente di apposito sistema antivirus aziendale, regolarmente ed automaticamente aggiornato nel tempo.

Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.

La segnalazione della presenza di eventuali virus, che eccezionalmente abbiano superato i controlli dell'antivirus, deve essere tempestivamente segnalata.

3.9. AUTORIZZAZIONE ALL'UTILIZZO DI DISPOSITIVI DI MEMORIZZAZIONE RIMOVIBILI

I supporti rimovibili sono affidati alla custodia dei soggetti autorizzati al trattamento dei dati personali.

L'utilizzo di supporti di memorizzazione rimovibili (es. hard disk esterni, CD ROM, DVD, chiavette USB o altri supporti magnetici/elettronici/ottici) è limitato al solo uso lavorativo per finalità di trasferimento di dati e documenti informatici.

Qualora tali supporti contengano dati non più utili, l'utente deve assicurarne la cancellazione sicura al termine dell'esigenza.

I supporti rimovibili devono essere comunque custoditi ed utilizzati in modo tale da impedire accessi non autorizzati da parte di terzi ed estrazione non consentita dei dati.

Possono essere utilizzati esclusivamente supporti di memorizzazione rimovibili che siano stati messi a disposizione o espressamente autorizzati dalla Società che potrà utilizzare sistemi automatici di blocco dei dispositivi non autorizzati.

Ogni dispositivo di memorizzazione di provenienza esterna, deve essere preventivamente controllato dall'antivirus prima dell'apertura di file in esso contenuti.

3.10. ORARI DI DISPONIBILITÀ DELLA RETE INFORMATICA

L'erogazione dei servizi IT è regolare e continuativa, ad eccezione delle interruzioni dovute ad interventi di manutenzione e riparazione.

In caso di interventi di manutenzione, programmata o per causa di forza maggiore, la Società si impegna ad adottare tutti i provvedimenti necessari al fine di ridurre al minimo il disagio per gli utenti.

Gli orari di accesso ai sistemi informativi aziendali sono garantiti in coerenza agli orari di lavoro degli uffici. L'orario di accesso remoto ai sistemi informativi aziendali è subordinato, previa autorizzazione ricevuta, all'utilizzo previsto.

3.11. TRASMISSIONE INFORMAZIONI

Al fine di prevenire eventuali accessi ai dati aziendali da parte di soggetti terzi non autorizzati, occorre adottare delle cautele nella trasmissione e riproduzione dei documenti contenenti dati personali. Quando le informazioni devono essere trasmesse telefonicamente occorre essere assolutamente certi dell'identità dell'interlocutore e verificare che esso sia legittimato ad ottenere quanto domandato.

Quando il dato deve essere inviato a mezzo fax, posta elettronica, SMS, ecc. occorre:

- prestare la massima attenzione affinché il numero telefonico o l'indirizzo e-mail immessi siano corretti;
- verificare che non vi siano inceppamenti di carta o che dalla macchina non siano presi più fogli e attendere sempre il rapporto di trasmissione per un ulteriore verifica del numero del destinatario e della quantità di pagine inviate;
- nel caso di documenti inviati per posta elettronica, accertarsi, prima di confermare l'invio, di avere allegato il file corretto;
- in caso di trasmissione di dati particolarmente delicati è opportuno anticipare l'invio chiamando il destinatario della comunicazione al fine di assicurare il ricevimento nelle mani del medesimo, evitando che terzi estranei o non autorizzati conoscano il contenuto della documentazione inviata.

Tutti coloro che provvedono alla duplicazione di documenti con stampanti, macchine fotocopiatrici o altre apparecchiature, in caso di copia erronea o non leggibile correttamente, da cui potrebbero essere desunti dati personali, sono tenuti a distruggere il documento in modo da escludere qualunque possibilità da parte di estranei di venire a conoscenza dei dati medesimi.

4. ATTIVITÀ DI CONTROLLO DEI SISTEMI

4.1. AUDITING DI SISTEMA

Le operazioni effettuate servendosi di userid e password possono essere memorizzate per finalità di sicurezza del sistema secondo quanto previsto dalla vigente normativa.

L'Azienda si riserva di utilizzare programmi per la protezione dalla navigazione in rete, di escludere la connessione con siti vietati o non attinenti agli scopi istituzionali della Società e di effettuare controlli, anche a campione, concernenti l'utilizzo corretto degli strumenti di lavoro.

Più in particolare tutte le attività di Auditing di Sistema (come verifiche circa l'improprio utilizzo della rete internet, della posta elettronica, etc.) verranno realizzate nel pieno rispetto della legislazione vigente, sia con riferimento al diritto del lavoro, ivi incluso ai sensi dell'art. 4 Legge n. 300/1970 come novellato dall'art. 23, comma 1, D.Lgs. 151/2015, che alla normativa che regola il trattamento dei dati, in particolare, ai provvedimenti dell'Autorità Garante per la protezione dei dati personali del 1 marzo 2007 (relativa alle linee guida per posta elettronica e internet) e del 27 novembre 2008 (relativa alle attribuzioni delle funzioni di amministratore di sistema).

Le violazioni relative all'utilizzo dei dispositivi aziendali e dei sistemi, rispetto a quanto contenuto nel presente documento, configurano illeciti che potranno comportare provvedimenti disciplinari secondo una gradualità in base alla gravità della condotta.

Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/Implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi relativi al traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà degli Amministratori di Sistema, accedere, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali e al documenti ivi contenuti.

4.2. ACCESSO AI DATI DELL'UTENTE A TUTELA DELLA PRIVACY

Poiché in caso di violazioni contrattuali e giuridiche, sia l'azienda, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, l'azienda verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico.

Ai sensi della vigente normativa in materia di privacy e, in particolare, in conformità a quanto disposto dal Provvedimento n. 13 del 1 marzo 2007 dell'Autorità Garante per la privacy, si ritiene necessario informare che:

- La cocietà, attraverso gli amministratori di sistema di sistema, effettua un monitoraggio non arbitrario, inutile o comunque discriminatorio dell'hardware e del software installato nei dispositivi informatici. Tale operazione viene effettuata, in modo completamente automatico per i dispositivi ed i sistemi operativi che lo consentono ed in modo manuale per tutti gli altri. Il monitoraggio, necessario per finalità organizzative (inventario del parco macchine e contabilità delle licenze d'uso del software), non coinvolge in alcun modo i dati personali ed i documenti presenti sui dispositivi, ma permette la rilevazione di software installato in violazione di questo disciplinare.

P.le Lombardia, 10 – 28100 Novara (NO)
P.I., C.F. 02443620030

- Gli Amministratori di Sistema possono accedere ai dati trattati dall'utente tramite posta elettronica o navigazione in rete esclusivamente per motivi di sicurezza e protezione del sistema Informatico (ad es., contrasto virus, malware, intrusioni telematiche, fenomeni quali spamming, phishing, spyware, etc.), ovvero per motivi tecnici e/o manutentivi e/o di regolare svolgimento dell'attività lavorativa (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware). Fatta eccezione per gli interventi urgenti che si rendano necessari per affrontare situazioni di emergenza e massima sicurezza, il personale incaricato accederà ai dati su richiesta dell'utente e/o previo avviso al medesimo.
- Ove sia necessario per garantire la sicurezza, l'assistenza tecnica e la normale attività operativa, il personale incaricato avrà anche la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni. Gli stessi amministratori di sistema possono, nei casi sopra indicati, procedere a tutte le operazioni di configurazione e gestione necessarie a garantire la corretta funzionalità del sistema informatico aziendale (ad es. rimozione di file o applicazioni pericolosi).
- In previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica delle caselle aziendali, l'utente può formalmente delegare un altro lavoratore (fiduciario) a verificare il contenuto dei messaggi, a gestire le strette necessità operative e/o ad inoltrare quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. In assenza della nomina di un fiduciario, l'Amministratore pro tempore della Società o persona da lui delegata, può legittimamente verificare il contenuto dei messaggi al fine di estrarre le informazioni ritenute rilevanti per lo svolgimento dell'attività lavorativa. Di tale attività verrà redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile.
- Al fine di prevenire, per quanto e ove possibile, comportamenti scorretti durante la navigazione in internet, l'azienda si avvale di appositi filtri che impediscono l'accesso a siti non ritenuti Idonei ed il download di file multimediali non attinenti all'attività lavorativa. Tali sistemi consentono anche la raccolta e la conservazione dell'attività di navigazione dei singoli utenti in appositi registri chiamati "file di log".
- L'eventuale controllo sui file di log da parte degli amministratori di sistema non è comunque continuativo ed è limitato ad alcune informazioni (es. Posta elettronica: l'indirizzo del mittente e del destinatario, la data e l'ora dell'invio e della ricezione e l'oggetto – Navigazione internet: Il nome dell'utente, l'identificativo della postazione di lavoro, indirizzo IP, la data e ora di navigazione, il sito visitato e il totale degli accessi effettuati) ed i file stessi vengono conservati per il periodo strettamente necessario per il perseguimento delle finalità di sicurezza dell'azienda, e comunque non oltre 12 mesi, fatti salvi in ogni caso specifici obblighi di legge. Il sistema di registrazione dei log è configurato per cancellare periodicamente ed automaticamente i dati personali degli utenti relativi agli accessi internet e al traffico telematico.
- Eventuali comportamenti anomali saranno segnalati genericamente alle aree interessate e, solo qualora tali comportamenti dovessero continuare, la Società potrà procedere, nel rispetto delle norme legali e contrattuali, a controlli individuali.
- Gli amministratori di sistema sono altresì autorizzati ad accedere ai dati contenuti negli strumenti informatici restituiti dall'utente all'azienda per cessazione del rapporto, sostituzione delle apparecchiature, etc. e a cancellarne i contenuti.

La Società garantisce la non effettuazione di alcun trattamento mediante sistemi hardware e software specificatamente preordinati al controllo a distanza.

4.3. SISTEMI DI CONTROLLI GRADUALI

In caso di anomalie, gli amministratori di sistema effettueranno controlli preliminari su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree che si concluderanno con avvisi generalizzati diretti ai dipendenti di detta struttura o aree in cui sia stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti aziendali e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie (come previsto dal p. 6.1 della Delibera Nr. 13 del 1/3/2007 Garante Privacy "lavoro: le linee guida del Garante per posta elettronica e internet").

In alcun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

5. CESSAZIONE DISPONIBILITÀ SERVIZI INFORMATIVI E MODALITÀ DI RESO

La disponibilità dei servizi informatici aziendali per il dipendente cesserà:

- qualora non sussista più la condizione di dipendente;
- qualora non fosse confermata l'autorizzazione all'uso fornita dalla Direzione.
- Il dipendente che vede cessata la disponibilità (totale o parziale) dei servizi informative dovrà:
- consegnare ogni bene aziendale in suo possesso, eventualmente comprensivo di accessori connessi e imballi originali;
- copiare, se fornito delle credenziali di accesso, sulle cartelle di rete condivise aziendali tutti gli eventuali dati di pertinenza aziendale;
- La Società provvederà a:
- attivare un risponditore automatico sulla casella di posta elettronica precedentemente concessa in uso all'incaricato; tale sistema resterà in funzione per 6 mesi, salvo accordi diversi, e comunicherà eventuali riferimenti alternativi; al termine del periodo previsto, la casella sarà disattivata;
- disattivare tutte le credenziali di autenticazione;
- effettuare il ripristino alla configurazione iniziale (reset / formattazione) dei dispositivi dotati di sistema operativo;

6. RISPETTO DELLE NORMATIVE AZIENDALI E LEGGI VIGENTI

È obbligo di tutto il personale dipendente attenersi alla presente procedura, alle altre normative aziendali e alle disposizioni di legge in materia di trattamento di dati/informazioni (Privacy, etc.).

7. PROVVEDIMENTI DISCIPLINARI

Il mancato rispetto o la violazione delle regole contenute nel presente documento è perseguibile con le sanzioni disciplinari previste dalla contrattazione collettiva o da accordi di secondo livello, nonché con le azioni civili, penali e contabili previste dalla normativa vigente.

Tutti gli utenti sono informati sugli ambiti di lavoro e sulla tipologia di informazioni a cui possono accedere. Ogni utente viene esplicitamente avvisato che il suo accesso è consentito solo alle aree di pertinenza formalmente autorizzate e documentate e, quindi, che eventuali accessi o tentativi di accesso ad aree non autorizzate potranno comportare provvedimenti nei suoi confronti.

L'eventuale illecito nell'utilizzo delle informazioni aziendali e della strumentazione informatica da parte dei dipendenti, può generare in capo all'azienda una serie di responsabilità, sia penali sia civili, qualora l'azienda stessa non dimostri di aver adottato le "giuste" precauzioni. Gli utenti devono essere consapevoli del danno per l'azienda conseguente alla perdita di informazioni, loro alterazione e/o compromissione della riservatezza, causato da comportamenti inadeguati, fraintendimenti, errori nelle valutazioni, incuranza, disattenzione, stanchezza, mancanza di motivazione, ecc.

Gli utenti devono anche essere consapevoli del fatto che gli amministratori di sistema hanno il diritto di accedere su tutti i sistemi, i computer e le apparecchiature aziendali e che l'azienda può raccogliere i "log" di tutte le transazioni, per gestire la qualità dei servizi informativi, per assicurare la rete aziendale, per garantire la sicurezza delle comunicazioni e la conformità alle normative, ai fini statistici e anche per controllare l'utilizzo delle risorse informative aziendali e il rispetto delle normative aziendali.

Se un dipendente o assimilato non rispetta le norme indicate in questo documento, i fatti rilevanti saranno portati (da parte del suo responsabile diretto e/o da parte degli amministratori di sistema) all'attenzione della Direzione Aziendale, che valuterà i fatti. L'azienda si riserva il diritto di esaminare tutte le informazioni conservate e trasmesse dai suoi sistemi e dalle sue reti. Questo monitoraggio può essere di natura globale, specifica o individuale.

Qualunque dipendente venga sorpreso in violazione sarà soggetto a provvedimenti disciplinari, nel rispetto della legislazione vigente in materia (in particolare, la contrattazione collettiva e lo Statuto dei lavoratori) che vanno dal richiamo verbale al licenziamento, in base alla gravità della materia.