DISCIPLINARE INFORMATICO AZIENDALE

Redatto in base alle disposizioni del

GENERAL DATA PROTECTION REGULATION (GDPR)

e

NORMATIVA NAZIONALE VIGENTE IN MATERIA DI PRIVACY

Indice

1. INTRODUZIONE E OBIETTIVI DELLA PROCEDURA

1.1. PRESENTAZIONE AZIENDALE E FINALITÀ DEL DIA (DISCIPLINARE INFORMATICO AZIENDALE)

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 definite e implementate dalla Società per 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 (c.d. RID);
- il trattamento dei soli dati personali necessari per ogni finalità di trattamento perseguita;
- la compliance alle normative cogenti esterne (internazionali, europee, nazionali e locali), nonché alle policy e alle procedure definite internamente dalla Società.

Tra gli obiettivi di dettaglio perseguiti dalla presente procedura troviamo quello di fornire agli addetti autorizzati, al personale tutto (interno ed esterno) che entra in contatto con il patrimonio informativo della Società, 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 prescrizioni adottate nel Modello di Organizzazione, Gestione e Controllo ex D.lgs. 231/01 ;
- delle disposizioni di cui agli artt. 2104 e 2105 codice civile;
- delle disposizioni dei CCNL;
- del General Data Protection Regulation (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;
- in generale, delle istruzioni fornite ed indicate al personale coinvolto nelle attività di trattamento di dati personali all'interno delle specifiche procedure redatte.

1.2. AMBITO DI APPLICAZIONE E PERIMETRO

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 intrattenuto, 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, un cellulare o altro dispositivo con connessione a Internet, nonché accesso a una casella di posta elettronica aziendale;
- abbiano accesso e/o 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.

In sintesi, le tre macroaree di sicurezza in perimetro, 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**: la funzione svolta dalla sicurezza fisica è quella di apprestare tutti i mezzi e gli strumenti necessari per proteggere persone, cose e ambienti dai suddetti rischi. Si suddivide in sicurezza d'area preordinata ad evitare accessi fisici non autorizzati e sicurezza delle apparecchiature hardware preordinata alla protezione da manomissione o furti dell'hardware e comprende anche la manutenzione degli stessi;
- **sicurezza Logica**: la funzione svolta dalla sicurezza logica è quella di proteggere i "dati" attraverso misure di sicurezza di carattere tecnologico. Rientrano in questa area i c.d. Sistemi di sicurezza preordinati alla protezione di tutte le piattaforme dati presenti in azienda (in primis mediante autenticazione e controllo accessi); meccanismi di sicurezza preordinati alla creazione del *modus operandi* dei sistemi di sicurezza (cifratura, firma digitale, meccanismi per l'autenticazione, ecc.);
- **sicurezza Organizzativa**: la funzione svolta dalla sicurezza organizzativa è quella di prevedere regole e procedure finalizzate a disciplinare gli aspetti organizzativi del processo di sicurezza fisica e logica. In questa area rientrano tutte le prescrizioni riguardanti la definizione dei ruoli, la distribuzione dei compiti e delle responsabilità. Quindi a titolo esemplificativo rientrano in questa area tutte le procedure relative alle procedure riguardanti il personale, le procedure di aggiornamento dei software, le procedure di backup etc.

Il DIA riguarda tutti i dati personali (sensibili, giudiziari e identificativi) trattati per mezzo di:

- strumenti elettronici di elaborazione;
- altri strumenti di elaborazione (ed esempio: Cartacei, Audio, Visivi e Audiovisivi, etc.).

1.3. ENTRATA IN VIGORE

Con l'entrata in vigore della presente procedura tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalla presente.

Copia del documento, oltre ad essere affisso nella bacheca aziendale, verrà pubblicato nella intranet aziendale e consegnato agli utenti in fase di assunzione.

2. TERMINI E DEFINIZIONI

Termine/Abbreviazione	Definizione
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.
RID	Riservatezza, Integrità e Disponibilità, ossia i tre requisiti fondamentali della sicurezza delle informazioni.
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 della 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 o dispositivo che utilizza sistemi d'elaborazione dei dati per ottenere o elaborare dati e per scambiare informazioni. Nel contesto della presente procedura, per utente deve intendersi ogni dipendente e 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 cliente o un altro soggetto interno o esterno ha il diritto di compiere una certa azione, ad es. di trasferire fondi o accedere a dati sensibili.
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, sia standard sia privilegiato (es. Amministratori di sistema), formalmente autorizzato dalla Società in qualità di Titolare, deve rispettare per garantire la sicurezza dei dati personali e delle informazioni aziendali in possesso, in gestione e/o sottoposte ad attività di trattamento da parte della Società.

3.1. CLASSIFICAZIONE DELLE INFORMAZIONI

Sono previste le seguenti classificazioni dei dati/documenti aziendali:

- **riservato**: informazioni gestionali rilevanti, accessibili solo al Vertice Aziendale;
- **confidenziale**: informazioni gestionali rilevanti accessibili al Vertice Aziendale e al Management Aziendale; su specifica autorizzazione del management l'accesso può essere consentito ai diretti dipendenti o su autorizzazione del Vertice anche a terzi.
- **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.

In ogni caso gli Utenti non sono autorizzati a divulgare all'esterno tali informazioni, salvo autorizzazione dei Responsabili.

3.2. AUTENTICAZIONE E QUALIFICAZIONE DELLE UTENZE

L'utilizzo dei servizi informatici aziendali richiede un codice di identificazione personale (*userid*) ed una parola chiave segreta (*password*), che non può essere ceduta a terzi, neppure temporaneamente.

Qualsiasi azione svolta sotto l'autorizzazione offerta dall'abbinamento *userid* e *password* 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.

L'Amministratore di sistema provvede a comunicare al nuovo utente la *userid* e la *password* per accedere. L'utente, al primo accesso, deve personalizzare la *password* secondo i criteri di sicurezza riportati nel successivo punto "Gestione delle Password".

La *password* deve:

- essere composta da almeno 5 caratteri;
- non contenere riferimenti agevolmente riconducibili all'utente;
- essere modificata al primo utilizzo e, successivamente, almeno ogni novanta giorni. Nel caso si sospetti che la *password* abbia perso la segretezza, dovrà essere immediatamente sostituita;
- ad ogni cambio *password* non sarà possibile impostare le 5 precedenti *password* utilizzate.

3.3. GESTIONE DELLE PASSWORD

3.3.1. LINEE GUIDA PER LA COSTRUZIONE DELLE PAROLE CHIAVE

L'accesso ad ogni postazione di lavoro individuale, alla rete e alle applicazioni aziendali avviene mediante *password* personali. Le *password* sono utilizzate per accedere a differenti profili di autorizzazione nell'ambito del sistema Informativo aziendale (es. utenze gestionale aziendale, accesso ad Internet, sistemi di posta elettronica, ecc..).

3.3.2. PAROLE CHIAVE DEBOLI

Le *password* di facile individuazione hanno le seguenti caratteristiche:

- si possono trovare in un comune dizionario italiano, inglese o altra lingua comune;
- sono parole di uso comune legate all'utente (nome di qualche membro della famiglia, di animali domestici, di amici, di collaboratori, ecc.);
- sono legate ad informazioni personali (date di nascita, indirizzi, numeri telefonici, ecc.);
- sono legate ad espressioni informatiche, *hardware* e *software*;
- sono sequenze ripetute del tipo "11111111", "22222222", "12121212", "12345678", ecc.

Sono considerate "deboli" anche le parole chiave precedentemente indicate, precedute o seguite da una cifra (giovanni1, 1giovanni, ecc.).

3.3.3. PAROLE CHIAVE SICURE

Sono da ritenere *password* di soddisfacente sicurezza quelle che hanno le seguenti caratteristiche:

- sono composte da caratteri maiuscoli e minuscoli;
- utilizzano anche caratteri di interpunzione, come ( ) ! ? • ",; ed una miscela di numeri e lettere.

Un altro importante accorgimento riguarda la selezione di parole chiave che possano essere facilmente digitate sulla tastiera, senza doverla guardare, per ridurre al minimo il tempo di digitazione ed evitare che la digitazione possa essere osservata da terzi nelle vicinanze.

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

3.3.4. PROTEZIONE DELLA PAROLA CHIAVE

Si raccomanda di non utilizzare la stessa *password* per sistemi di autenticazione interni all'Azienda e per sistemi di autenticazione esterni (ad esempio: l'accesso al proprio conto corrente bancario) non legati all'attività aziendale.

Ove ad un incaricato vengano attribuiti diversi profili di autorizzazione, non deve essere usata la stessa *password* (ad esempio: deve essere scelta una *password* per l'accesso all'area tecnica del sistema, ed una *password* differente e separata per l'accesso al gestionale).

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

3.4. GESTIONE ED USO DELLE DOTAZIONI AZIENDALI

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

Ogni rottura sarà oggetto di valutazione da parte della Società per verificarne la natura ed eventualmente, in caso di comportamenti non adeguati, adottare ulteriori provvedimenti.

L'utilizzo di cd rom, cd riscrivibili, nastri magnetici, chiavi USB (o altri dispositivi) per la memorizzazione di informazioni aziendali è generalmente vietato; qualora necessario, deve essere autorizzato dall'Ufficio del Personale.

3.4.1. FURTI E GUASTI DI APPARATI

Stante la vigenza di quanto sopraindicato, in caso di furto, il dipendente è tenuto a sporgere denuncia all'autorità di competenza e presentarne copia alla Società, nonché dare avvio a quanto riportato nel paragrafo 3.19 SEGNALAZIONE ANOMALIE/INCIDENTI DI SICUREZZA del presente documento.

3.4.2. SERVIZIO DI ASSISTENZA PER LA TELEFONIA MOBILE

Il servizio di telefonia mobile prevede l'assistenza tecnica sugli apparati di telefonia mobile, dati e schede SIM.

Tramite email saranno concordate le modalità di consegna.

3.5. 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.

Al termine del trattamento o una volta esaurite le finalità per i dati erano stati raccolti, i documenti in cui essi sono contenuti devono essere resi non più intellegibili tramite appositi strumenti (es. trita-documenti).

3.6. 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 è proibito e potrà essere sanzionato poiché può contribuire ad innescare disservizi, costi di manutenzione e minacce alla sicurezza.

Tutti i file devono essere conservati in cartelle di rete condivise, messe a disposizione di ogni dipendente ed opportunamente configurate all'uso dai responsabili IT. Tali cartelle sono definite secondo criteri di gruppo e collaborazione, sia a livello di funzione che a livello di servizio. Sui sistemi che ospitano tali cartelle sono definite periodiche attività di backup schedulate.

L'archiviazione su disco locale deve essere esclusivamente temporanea ed occasionale. Tutta la documentazione aziendale utilizzata dai dipendenti per scopi lavorativi deve essere quotidianamente conservata nelle cartelle condivise precedentemente descritte.

Dovranno essere effettuati periodici backup dei dati aziendali, provvedendo a conservare il dato nelle opportune cartelle di rete per la condivisione con altri utenti autorizzati al relativo trattamento.

In ogni caso, attenendosi ai comportamenti precedentemente definiti, prevedendo che i dischi locali delle postazioni di lavoro non contengano dati aziendali, ogni eventuale rottura del disco locale non prevedrà, da parte dell'Azienda, il recupero dei dati, ma solamente la sostituzione dello stesso.

È vietato l'uso di programmi diversi da quelli ufficialmente installati dal personale IT 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 espone 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 libero e quindi non protetto da detta normativa, vengono sanzionate anche penalmente.

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 (assicurando gli opportuni controlli).

Tutti i file di provenienza esterna (ricevuti tramite posta elettronica, navigazione Internet o presenti su dispositivi USB collegati direttamente alle postazioni di lavoro), sono sottoposti a controlli automatici garantiti da tecnologie *hardware* e *software*, coordinati dai responsabili IT.

3.7. POSTAZIONE DI LAVORO PORTATILE (LAPTOP)

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 al precedente punto, con particolare attenzione alla rimozione di eventuali file elaborati prima della riconsegna.

Per ridurre i rischi nell'uso di tali dispositivi sarà cura dell'utente ricollegare alla rete aziendale, almeno mensilmente, la postazione portatile assegnata al fine di assicurarsi che:

- l'antivirus aziendale installato sia aggiornato e attivato;
- siano installate le *patch* di sicurezza del sistema operativo e dei prodotti *software* utilizzati.

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 i responsabili IT potranno attivare password di accesso controllato di basso livello (es. Bios) e/o la crittografia del disco fisso.

3.8. GESTIONE DEGLI ACCESSI ALLA RETE INTERNET E Al RELATIVI SERVIZI

Gli accessi alla rete interna, 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 interna deve avvenire esclusivamente tramite dispositivi di sicurezza forniti dalla Società.

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 gratuiti (*freeware*) e *shareware*, 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 venir a tal fine contattato il personale IT);
- 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 dal Responsabile.

Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, la Società rende peraltro nota l'adozione di uno specifico sistema di blocco o filtro automatico che prevenga determinate operazioni quali *l'upload*, il *download* o l'accesso a determinati siti inseriti in una *blacklist*.

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;

3.9. SERVIZI DI POSTA ELETTRONICA

A tutti i dipendenti è fornita una casella di posta elettronica interna individuale (ovvero in taluni casi di gruppo) che dovrà essere utilizzata esclusivamente per ragioni inerenti l'attività lavorativa; ogni dipendente è responsabile del corretto utilizzo, che non comprende la partecipazione a dibattiti, forum, etc..

Il dipendente può accedere alla sua casella di posta elettronica da tutti gli strumenti che utilizza (Desktop, Laptop, Tablet, Telefono Mobile). Gli strumenti dovranno essere dotati dei minimi requisiti di sicurezza definiti dal presente documento; il personale IT può richiedere l'eventuale installazione di appositi applicativi di sicurezza limitatamente alla posta elettronica con account aziendale per quanto riguarda i telefoni mobili.

Nell'utilizzo del servizio ciascun utente è tenuto ad attivare, in caso di assenza prolungata, la funzione di risposta automatica che inviti il mittente a prendere contatto con altre risorse della Società.

La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e allegati ingombranti.

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 a ciascun utente, secondo le prassi aziendali. Tali messaggi sono archiviati automaticamente su sistemi di archiviazione aziendale.

Tutti i messaggi, siano essi inviati o ricevuti, presenti all'interno delle caselle di posta elettronica aziendale, vengono quotidianamente sottoposti a processi di conservazione, utilizzando gli strumenti software preposti.

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

Il loro utilizzo è consentito esclusivamente al destinatario 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 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 o *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 al personale IT. Non si dovrà in alcun caso procedere all’apertura degli allegati a tali messaggi.

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 (cfr. 5.17.2).

L’Amministratore di Sistema, qualora ravveda situazioni particolarmente gravi e/o abusi del servizio, è tenuto ad informare la Direzione Aziendale che provvederà alla contestazione delle mancanze rilevate.

3.10. CONFIGURAZIONI HARDWARE/SOFTWARE

Le configurazioni delle postazioni di lavoro e degli altri strumenti hardware e software vengono eseguite dalla Società.

I responsabili IT possono autorizzare l’installazione di ulteriori programmi informatici sul PC del dipendente, su richiesta scritta del Responsabile dell’Area in cui opera il dipendente.

Nel caso di assegnazione/restituzione di PC portatile, Il dipendente si incarica di rimuovere eventuali file memorizzati sullo stesso prima della riconsegna.

3.11. UTILIZZO DEI TELEFONI FISSI, FAX E FOTOCOPIATRICI

Il telefono aziendale affidato all’utente è uno strumento di lavoro. Ne viene concesso l’uso esclusivamente per lo svolgimento dell’attività lavorativa, non essendo quindi consentite comunicazioni non strettamente inerenti l’attività lavorativa stessa.

È vietato l’utilizzo dei fax aziendali per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte del Responsabile di ufficio.

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

3.12. UTILIZZO DISPOSITIVI MOBILI (SMARTPHONE/TABLET)

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 mobili non possono essere ceduti né fatti utilizzare a terzi, eccetto colleghi, collaboratori, consulenti o soggetti autorizzati.

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 pirata, 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 dalla Direzione.

L'utilizzatore che abbia necessità di apportare modifiche *software* o *hardware* al dispositivo mobile In dotazione, installando nuovi programmi o dispositivi, deve farne preventiva richiesta ai responsabili IT.

L'utente, ove possibile, deve mantenere aggiornato il sistema operativo e le *app* del dispositivo mobile attraverso le comuni procedure di *software update* messe a disposizione dai *Vendor*.

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 periferica Wi-Fi va abilitata sul dispositivo mobile solo ed esclusivamente ai fini d'accesso alla rete aziendale e/o di altre reti protette. Non va mai lasciato inutilmente attivo. In caso di guasti o malfunzionamenti, l'utilizzatore dovrà rivolgersi ai responsabili IT a cui è demandata la relativa gestione in queste circostanze.

I responsabili IT possono disporre dei dispositivi mobili secondo necessità, sostituendo, aggiornando, rimuovendo o adeguando in tutto o in parte le componenti *hardware* e/o *software* di cui essi si compongono, senza necessità di preavviso e di richiesta di consenso da parte dell'utilizzatore.

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.

Qualora fossero individuati componenti *hardware* e/o *software* (programmi, documenti, dispositivi esterni, etc.) non corrispondenti ai criteri di sicurezza e di operatività individuati dai responsabili IT o non esplicitamente autorizzati, tali

componenti potrebbero essere rimossi e l'utilizzatore potrebbe essere coinvolto negli accertamenti e nelle verifiche del caso.

3.13. 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 necessario utilizzare la propria *password* ed il proprio nome utente.
È richiesta agli utenti, per quanto di loro competenza, la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei *file* obsoleti, duplicati o non più utili.

3.14. PROTEZIONE ANTIVIRUS E AUTORIZZAZIONE ALL'UTILIZZO DI DISPOSITIVI DI MEMORIZZAZIONE RIMOVIBILI

Il personale IT provvedono all'installazione sulla postazione di lavoro assegnata (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 a cura dell'utente alla struttura suddetta.

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 e di *backup* di dati e documenti informatici.

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

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 dalla Società ed espressamente autorizzati dalla Direzione.

Ogni dispositivo di memorizzazione di provenienza esterna (*hard disk* esterni, cd rom, cd riscrivibili, nastri magnetici, chiavi USB o altri dispositivi) deve essere controllato dall'antivirus; l'utente deve assicurarsi, in tali casi, che l'antivirus sia regolarmente installato sulla postazione di lavoro.

3.15. 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.

3.16. 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 giusto;
- 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.

3.17. ATTIVITÀ DI CONTROLLO DEI SISTEMI

3.17.1. 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, l'improprio utilizzo 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 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 di connessione ad internet, traffico telefonico, etc.}, comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà dell' Amministratore di Sistema, anche tramite i propri incaricati, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali e al documenti ivi contenuti.

3.17.2. 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 dalla Provvedimento n. 13 del 1 marzo 2007 dell'Autorità Garante per la privacy, si ritiene necessario informare che:

- La Direzione Aziendale, attraverso gli Amministratori 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.
- L'Amministratore di Sistema può 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 esempio, 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. Lo stesso Amministratore di Sistema e/o i suoi incaricati possono, nei casi su 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 del 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, da effettuarsi entro tempi adeguati per l'espletamento della richiesta avanzata da parte del Responsabile d'ufficio, con la presenza di quest'ultimo e di personale appositamente incaricato (ad esempio gli amministratori dei sistemi o della Direzione competente in materia), il Titolare 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 dell'Amministratore 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 (attraverso procedure di sovra registrazione) 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 Direzione potrà procedere, nel rispetto delle norme legali e contrattuali, a controlli individuali.
- L'Amministratore di Sistema e i suoi incaricati sono altresì abilitati 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.

Nell'ambito delle misure di controllo del livello di sicurezza del sistema informativo, è possibile che l'Amministratore di Sistema o persona da lui delegata, effettui tentativi di violazione delle *password* degli utenti. Nel caso il tentativo abbia esito positivo, verrà chiesto all'utente di sostituire immediatamente la *password*.

3.17.3. SISTEMI DI CONTROLLI GRADUALI

In caso di anomalie, il personale IT effettuerà 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.

3.18. 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 dal Responsabile.

Il dipendente che vede cessata la disponibilità (totale o parziale) dei servizi informativi a lui dedicati dovrà:

- consegnare ogni bene aziendale in suo possesso, eventualmente comprensivo di accessori connessi e imballi originali, entro 1 ora dal termine del rapporto, ovvero dalla ricezione dell'annullata autorizzazione all'utilizzo;
- copiare sulle cartelle di rete condivise aziendali tutti gli eventuali dati di pertinenza aziendale;
- cancellare preventivamente tutti gli eventuali dati personali eventualmente ivi contenuti.

Nel caso dei dispositivi *mobile* è compito della funzione preposta:

- effettuare il ripristino alla configurazione iniziale (*reset*) dei dispositivi mobile aziendali dotati di sistema operativo;
- attivare un risponditore automatico sulla casella di posta elettronica precedentemente concessa in uso all'incaricato: tale sistema entrerà in funzione per la durata di 1 mese, salvo accordi diversi, e comunicherà eventuali riferimenti alternativi; al termine del periodo previsto, la casella sarà disattivata;
- disattivare le credenziali di autenticazione sui server.

3.19. SEGNALAZIONE ANOMALIE/INCIDENTI DI SICUREZZA

Qualsiasi anomalia o incidente per la sicurezza delle informazioni deve essere sempre segnalato alle persone e con le modalità indicate nella Policy del data Breach ovvero nella specifica procedura aziendale di gestione degli incidenti IT . Sono considerati incidenti di sicurezza IT tutti gli incidenti che riguardano la sicurezza di dati, informazioni e risorse IT (HW, SW, apparecchiature) e che compromettono, anche parzialmente, la riservatezza dei dati, l'integrità delle informazioni (es. errori causati da dati incompleti o inesatti), la disponibilità dei servizi informativi (es. problemi di sistema e perdite di servizio), l'ottemperanza alle normative (es.: privacy, copyright, ecc.).

Qualsiasi situazione a rischio e qualsiasi sospetto di carenza nella sicurezza devono essere segnalati tempestivamente al proprio Responsabile diretto. Nei casi particolari di incidenti o situazioni a rischio che possono essere considerati "confidenziali", la notizia va mantenuta riservata, altrimenti l'indagine rischia di essere fuorviata. Il Responsabile diretto, a sua volta, deve avvisare la Direzione Aziendale.

4. 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.).

4.1. 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 utente interno 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.

In caso di furto o smarrimento o danneggiamento di dispositivi mobili, non è esclusa a priori la responsabilità dell'utilizzatore nel sostenere, anche solo in parte, i costi per la riparazione o sostituzione del dispositivo mobile.

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.