Regolamento per l'utilizzo dei sistemi informatici e delle banche dati cartacee di SimplyIT

Sommario

Premessa

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete Internet dai Personal Computer, espone **SimplyIT**, con sede legale in Loreggia (PD), Via Guizze alte 7/D, e-mail privacy@simplyit.it (di seguito la "Società") e gli utenti a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge sul diritto d'autore e legge sulla privacy, fra tutte), creando evidenti problemi alla sicurezza ed all'immagine dell'azienda stessa.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si seguono nell'ambito dei rapporti di lavoro, la Società ha deciso di adottare il presente Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problematiche o minacce alla sicurezza nel trattamento dei dati.

Considerato inoltre che la Società, nell'ottica di uno svolgimento proficuo e più agevole della propria attività, può decidere, in alcuni casi, di mettere a disposizione dei propri dipendenti e collaboratori che ne necessitino per il tipo di funzioni svolte, mezzi di comunicazione efficienti (computer, portatili, telefoni cellulari, ecc.), sono state inserite nel presente Regolamento alcune previsioni relative alle modalità ed ai doveri che ciascun dipendente deve osservare nell'utilizzo di tale strumentazione.

Il presente regolamento rappresenta parte integrante delle informazioni fornite ai dipendenti e terze parti utenti, ai sensi dell'art. 13 del Regolamento UE 2016/679 ("Regolamento Privacy") con particolare riguardo al trattamento dei dati personali che la Società potrebbe effettuare in relazione all'utilizzo da parte di dipendenti delle risorse informatiche aziendali (personal computer, smart-phone, tablet, risorse di rete, stampanti, periferiche, ecc.), della posta elettronica aziendale e della navigazione in Internet.

1. Entrata in vigore e pubblicità

1.1. Il presente Regolamento, nella versione aggiornata alla data indicata in calce, entrerà in vigore da tale data. Con l'entrata in vigore del presente Regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.

1.2. Copia del presente Regolamento, oltre ad essere affisso nella bacheca aziendale ed inserito nell'apposito drive dedicato e condiviso denominato "Regolamenti aziendali personale SimplyIT", verrà consegnato a ciascun dipendente.

2. Destinatari

2.1. Il presente Regolamento si applica a tutti i dipendenti e collaboratori ai quali sono affidati cespiti aziendali o altre attrezzature di proprietà o nella disponibilità della Società per lo svolgimento delle proprie mansioni, indipendentemente dal ruolo o livello. Si applica inoltre ai collaboratori esterni che, nell'ambito del proprio rapporto contrattuale, abbiano accesso alle risorse informatiche della Società mediante credenziali di autenticazione dedicate.

2.2. Ai fini delle disposizioni relative all'utilizzo delle risorse informatiche e telematiche, per "utente" si intende qualsiasi dipendente o collaboratore, inclusi, a titolo esemplificativo, lavoratori somministrati, stagisti, apprendisti, consulenti e società esterne, in possesso di specifiche credenziali di autenticazione. Tale figura può essere altresì indicata come "designato al trattamento".

3. Utilizzo delle risorse informatiche

3.1. La Società è esclusiva titolare e proprietaria dei device aziendali, inclusi quelli acquisiti a seguito di contratti di noleggio e messi a disposizione degli utenti per l'attività lavorativa. In particolare, l'utilizzo promiscuo, ossia l'impiego dei dispositivi per scopi personali o comunque non strettamente legati all'attività lavorativa, è vietato, salvo espressa e preventiva autorizzazione della Società secondo le modalità indicate nel presente Regolamento. La Società è altresì unica titolare di tutte le informazioni, registrazioni e dati contenuti o trattati mediante i propri device digitali, archiviati in forma cartacea nei propri locali o conservati nella posta elettronica aziendale. L'utente non potrà ritenere che le informazioni, le registrazioni e i dati da lui trattati o memorizzati (inclusi messaggi di posta elettronica, chat, file di immagini, filmati o altre tipologie di file) abbiano natura privata o personale, né che tali dati possano essere copiati, comunicati o diffusi senza l'autorizzazione della Società. Le risorse informatiche (personal computer, smartphone, tablet, risorse di rete, stampanti, periferiche, ecc.) affidate all'utente sono strumenti di lavoro e, per i collaboratori, strumenti forniti dalla Società per l'esecuzione del rapporto contrattuale professionale. Di conseguenza, ogni utilizzo non inerente all'attività lavorativa e/o professionale è vietato, in quanto potrebbe provocare disservizi, costi di manutenzione non preventivati e, soprattutto, minacciare la sicurezza. Qualsiasi eventuale tolleranza da parte della Società, apparente o effettiva, non potrà legittimare comportamenti in contrasto con le disposizioni del presente Regolamento.

3.2. I device aziendali devono essere utilizzati con la necessaria diligenza e correttezza e devono essere custoditi con cura evitando ogni possibile forma di danneggiamento.

3.3. I device aziendali, dati in affidamento all'utente, permettono l'accesso alla rete della Società solo attraverso specifiche credenziali di autenticazione come meglio descritto al successivo punto 4 del presente Regolamento.

3.4. La Società rende noto che personale appositamente designato dalla Società stessa è autorizzato a compiere interventi nel sistema informatico aziendale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware ecc.). Detti interventi, anche in considerazione dei divieti di cui ai successivi punti n. 8.3, 9.1 e 9.2, potranno comportare l'accesso ai dati trattati dall'utente, ivi compresi i dati presenti negli archivi di posta elettronica aziendale, nonché la verifica – nel più assoluto rispetto delle prescrizioni indicate nelle Linee guida del Garante Privacy per posta elettronica e internet del 1° marzo 2007, in caso di utilizzo di personal computer e device aziendali – dei siti internet nei quali gli utenti abilitati alla navigazione esterna hanno accesso.

3.5. In ragione di quanto specificato al precedente paragrafo 3.4., il personale designato ha la facoltà di collegarsi e visualizzare da remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, ecc. L'intervento viene effettuato su richiesta dell'utente ovvero, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione preventiva all'utente della necessità dell'intervento stesso.

3.6. Non è consentito l'uso di programmi diversi da quelli installati dal personale designato dalla Società nel device assegnato all'utente; né è consentito agli utenti 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, tra l'altro, la Società al rischio di gravi responsabilità; si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore sul software, che impone la presenza nel sistema di software regolarmente licenziato o comunque non protetto dal diritto d'autore, vengono sanzionate anche penalmente.

3.7. E' fatto divieto assoluto di collegare alla rete aziendale risorse informatiche private (ivi inclusi personal computer fissi o portatili), ove detto collegamento non sia stato preventivamente ed espressamente autorizzato dalla Società.

3.8. Salva preventiva espressa autorizzazione del personale designato dalla Società, non è consentito all'utente modificare le caratteristiche impostate sui propri device né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ecc.).

3.9. L'utente, ove autorizzato, deve in ogni caso prestare la massima attenzione ai supporti di origine esterna che utilizza ed avvertire immediatamente il personale designato dalla Società nel caso in cui siano rilevati virus adottando quanto previsto dal successivo punto 10 del presente Regolamento relativo alle procedure di protezione antivirus.

3.10. Al termine della giornata lavorativa, è fatto obbligo di chiudere la propria sessione di lavoro sul Personal Computer e su ogni altro dispositivo utilizzato. In caso di suo inutilizzo per abbandono momentaneo della postazione utente, il Personal Computer dovrà essere bloccato secondo procedure (è consigliato agli utenti di impostare lo screensaver automatico dopo 1 minuto di inutilizzo).

3.11. A seguito della cessazione del rapporto lavorativo e/o professionale dell'utente con la Società o, comunque, al venir meno, ad insindacabile giudizio della Società, della permanenza dei presupposti per l'utilizzo dei device aziendali, gli utenti hanno i seguenti obblighi:

- procedere immediatamente alla restituzione dei device in uso;
- astenersi dal formattare o alterare o manomettere o distruggere i device assegnati o rendere inintelligibili i dati in essi contenuti tramite qualsiasi processo.

All'atto della consegna del device e a sindacabile giudizio della Società potrà essere predisposta una copia dei contenuti del device che verrà mantenuta per il tempo necessario in relazione ai relativi obblighi contrattuali e/o di legge, fatte salve specifiche ulteriori esigenze, ai fini di garantire alla Società l'utilizzo dei dati per interesse legittimo quale tutela dei diritti in sede giudiziaria.

3.12. A seguito di una cessazione del rapporto lavorativo o di consulenza dell'addetto con la Società o, comunque, al venir meno, ad insindacabile giudizio della Società, della permanenza dei presupposti per l'utilizzo di dati cartacei aziendali, gli incaricati hanno i seguenti obblighi:

- procedere immediatamente alla restituzione dei dati cartacei in loro possesso;
- divieto assoluto di alterare o manomettere o distruggere i dati cartacei assegnati o renderli inintelligibili tramite qualsiasi processo.

4. Gestione ed assegnazione delle credenziali di autenticazione per l'accesso alla rete

4.1. Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal personale designato dalla Società.

4.2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), associato ad una parola chiave (password) riservata che dovrà essere custodita dall'utente con la massima diligenza e non divulgata. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte del personale designato dalla Società.

4.3. La parola chiave, formata da lettere maiuscole e minuscole, numeri e simboli, in combinazione fra loro, deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'utente.

4.4. È necessario procedere alla modifica della parola chiave a cura dell'utente al primo utilizzo e, successivamente, almeno ogni sei mesi.

4.5. Qualora la parola chiave dovesse venir sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, si procederà in tal senso d'intesa con il personale designato dalla Società.

4.6. Per una corretta e sicura gestione della propria password l'utente deve, tra l'altro, rispettare le regole seguenti:

- le password sono assolutamente personali e non vanno mai comunicate ad altri;
- occorre cambiare immediatamente una password non appena si abbia alcun dubbio che sia diventata poco "sicura";
- le password non devono essere memorizzate su alcun tipo di supporto, quali, ad esempio, Post-It (sul monitor o sotto la tastiera) o agende (cartacee, posta elettronica, telefono cellulare);
- le password devono essere sostituite almeno nei tempi indicati dalla Società, a prescindere dall'esistenza di un sistema automatico di richiesta di aggiornamento password;
- evitare di digitare la propria password in presenza di altri soggetti che possano vedere la tastiera, anche se collaboratori o dipendenti della Società.

5. Utilizzo della rete della Società

5.1. Per l'accesso alla rete della Società ciascun utente deve essere in possesso delle specifiche credenziali di autenticazione.

5.2. È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le parole chiave d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.

5.3. Le cartelle utenti presenti nei server della Società sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato su queste unità, sulle quali vengono svolte regolari attività di controllo, amministrazione e back-up da parte del personale designato dalla Società. Anche i dischi o altre unità di memorizzazione locali (es. disco C: interno PC) sono soggetti a salvataggio da parte del personale designato dalla Società.

5.4. Il personale designato dalla Società può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericoloso per la sicurezza.

5.5. Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

6. Utilizzo e conservazione dei supporti rimovibili

6.1. L'utilizzo e conservazione di dati su supporti rimovibili è ammessa solo previa ed espressa autorizzazione della Società. Tutti i supporti magnetici rimovibili (CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati personali e/o sensibili nonché informazioni costituenti know-how aziendale, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere comunicato a terzi, trafugato e/o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

6.2. Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili e/o aventi natura particolare, ciascun utente dovrà contattare il personale designato dalla Società e seguire le istruzioni da questo impartite.

6.3. In ogni caso, i supporti magnetici contenenti dati sensibili e/o di natura particolare devono essere adeguatamente custoditi dagli utenti in cassetti/armadi chiusi.

6.4. E' vietato l'utilizzo di supporti rimovibili personali.

6.5. L'utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.

7. Utilizzo di Personal Computer portatili e/o altri dispositivi

7.1. Responsabilità

Il Personal Computer (PC) fornito dall'azienda, così come qualsiasi altro dispositivo o accessorio in affidamento (ad esempio, mouse, ricevitori Bluetooth, caricabatterie, ecc.), è uno strumento di lavoro. Ogni dipendente è responsabile della sua custodia e del suo utilizzo. Qualsiasi utilizzo non correlato all'attività lavorativa è vietato, poiché può generare disservizi, costi di manutenzione e minacce alla sicurezza. Il PC e tutti gli accessori assegnati devono essere custoditi con cura per evitare danneggiamenti, personalizzazioni inappropriate, incuria e smarrimento.

7.2. Protezione e Sicurezza degli Asset

Ogni dipendente è responsabile di proteggere gli asset informatici assegnati, inclusi PC e accessori, da accessi non autorizzati, modifiche, perdite o danni. Le misure di protezione includono la non divulgazione delle credenziali personali, l'uso responsabile di supporti esterni e la comunicazione immediata al Responsabile per la gestione dei sistemi informatici aziendali in caso di rilevazione di virus, problemi di sicurezza o malfunzionamenti.

7.3. Gestione degli Asset in caso di Incuria, Smarrimento o Furto

I dipendenti devono adottare tutte le misure appropriate per prevenire l'incuria, lo smarrimento e il furto degli asset informatici, inclusi PC, mouse, ricevitori Bluetooth e altri accessori. È vietato lasciare i dispositivi incustoditi o fuori dalla vista, specialmente se non adeguatamente bloccati o spenti. È inoltre vietato lavorare da luoghi pubblici non controllati o a rischio (es. parchi, caffetterie) per evitare situazioni di pericolo o potenziali furti. In caso di smarrimento di componenti minori, come un mouse o un ricevitore Bluetooth, il dipendente sarà direttamente responsabile della sostituzione a proprie spese con un dispositivo identico o equivalente. In caso di furto o smarrimento del PC o di altri dispositivi, il dipendente deve informare tempestivamente il proprio diretto Responsabile e il reparto IT, oltre a denunciare l'accaduto alle Forze dell'Ordine, fornendo alla Società una copia dell'atto di denuncia. La sostituzione del dispositivo avverrà solo dopo la comunicazione della denuncia di smarrimento o furto. Tuttavia, è importante notare che non tutte le casistiche di furto sono coperte dall'assicurazione aziendale. Ad esempio, furti con destrezza (es. sottrazione del dispositivo in spazi pubblici senza uso di forza) o situazioni in cui il dispositivo è stato lasciato incustodito in un luogo non sicuro non saranno coperti dall'assicurazione. In tali casi, la Società si riserva di addebitare al dipendente sarà tenuto il 50% del costo di un nuovo dispositivo equivalente, indipendentemente dal fatto che la situazione sia coperta o meno dall'assicurazione aziendale.

7.4. Utilizzo e Scambio di Materiale Aziendale

I dispositivi e gli accessori assegnati a un dipendente sono destinati esclusivamente all'uso professionale di quel dipendente. È vietato prendere in prestito o utilizzare materiale informatico o altri dispositivi assegnati ad altri colleghi senza previa autorizzazione scritta da parte del Responsabile diretto e del Responsabile per la gestione dei sistemi informatici aziendali. Inoltre, non è consentito lo scambio o il trasferimento di dispositivi o accessori tra colleghi senza il consenso esplicito dell'Ufficio IT. L'utilizzo non autorizzato o lo scambio di materiale tra dipendenti può compromettere la sicurezza aziendale e creare situazioni di responsabilità non tracciate.

7.5. Manutenzione e Smaltimento degli Asset

I dipendenti sono tenuti a mantenere i propri PC e accessori in buono stato, effettuando pulizie periodiche e rimuovendo file obsoleti o non necessari. Il Responsabile per la gestione

dei sistemi informatici aziendali è autorizzato a eseguire interventi di manutenzione, aggiornamento e sostituzione degli asset informatici, garantendo la sicurezza e l'integrità del sistema. In caso di cessazione del rapporto di lavoro o di collaborazione, i dipendenti devono rimuovere e cancellare eventuali file personali presenti sui dispositivi aziendali prima di riconsegnarli.

7.6. Cessione dei Beni Aziendali

In via generale, la cessione a qualsiasi titolo dei beni aziendali ai dipendenti, inclusi PC, tablet, accessori e altri dispositivi, non è consentita in alcuna circostanza, neanche a fine rapporto di lavoro. Tale dispositiva include dipendenti e non. Questa politica è motivata da una serie di ragioni amministrative, contabili e operative:
Proprietà e Tracciabilità: I beni aziendali sono di proprietà della Società e possono essere soggetti a contratti di noleggio, leasing o altre forme di finanziamento che ne limitano la libera disponibilità. La cessione a titolo gratuito potrebbe violare tali contratti e complicare la tracciabilità e la gestione degli asset aziendali. Difficoltà nella Gestione Contabile: La cessione a titolo gratuito o la vendita a prezzo simbolico di beni aziendali può creare complessità contabili e amministrative. Potrebbe risultare difficile per la Società giustificare tali operazioni senza incorrere in problematiche fiscali o legali, soprattutto in presenza di beni ammortizzabili. Gestione del Valore Residuo: I beni aziendali possono avere un valore residuo significativo anche dopo l'utilizzo interno. La cessione potrebbe impedire alla Società di recuperare tale valore attraverso canali appropriati, come la rivendita a terzi, il riciclo o la redistribuzione interna. Sicurezza e Riservatezza dei Dati: La cessione di dispositivi aziendali che contengono o hanno contenuto informazioni sensibili potrebbe rappresentare un rischio per la sicurezza dei dati. Anche con la rimozione dei dati, non si può garantire al 100% la protezione contro la possibile recuperabilità delle informazioni. Standard di Conformità e Audit: La cessione di beni aziendali potrebbe compromettere la conformità a standard interni o normativi, rendendo complicata la gestione degli audit e delle verifiche periodiche sugli asset aziendali. Per questi motivi, tutti i beni aziendali devono essere restituiti alla Società al termine del rapporto di lavoro, in condizioni adeguate e senza ritardi ingiustificati. L'inosservanza di queste disposizioni può portare a sanzioni disciplinari, inclusa la trattenuta di eventuali costi aggiuntivi sui compensi finali del dipendente.
Fermo quanto sopra, in via del tutto eccezionale e a proprio insindacabile giudizio, la Società può riservarsi di valutare la cessione al dipendente di beni aziendali.

7.7. Best practices per la condivisione di informazioni con l'esterno

Nel corso delle attività lavorative, potrebbe essere necessario condividere informazioni con soggetti esterni all'azienda, come clienti, fornitori o partner. Per garantire la sicurezza delle informazioni e il rispetto delle normative sulla privacy, è importante seguire le seguenti best practices:

Condividere solo le informazioni strettamente necessarie: Quando si condividono informazioni con soggetti esterni, assicurarsi di fornire solo le informazioni strettamente necessarie per lo scopo richiesto. Evitare la divulgazione di informazioni riservate o sensibili senza un motivo valido.

Utilizzare metodi di condivisione sicuri: Quando si condividono informazioni con l'esterno, utilizzare metodi di condivisione sicuri e protetti, come il trasferimento crittografato dei dati o l'utilizzo di portali sicuri per l'accesso alle informazioni.

Verificare l'identità del destinatario: Prima di condividere informazioni con soggetti esterni, assicurarsi di verificare l'identità del destinatario e di avere l'autorizzazione necessaria per condividere le informazioni con tale persona o entità.

Proteggere le informazioni con password o crittografia: Quando si condividono documenti o file contenenti informazioni sensibili, proteggerli con password o crittografia per ridurre il rischio di accesso non autorizzato.

Utilizzare sistemi di controllo documentale e condivisione con scadenza: Quando si condividono informazioni, utilizzare sistemi che consentono il controllo documentale e la scadenza dei documenti condivisi, come link a scadenza. Evitare l'utilizzo del mezzo e-mail per la condivisione di documenti, a meno che non sia necessario ai fini della storicizzazione di uno scambio esterno di informazioni in modo strutturato e per la tracciabilità dell'informazione.

Documentare la condivisione delle informazioni: Tenere traccia delle informazioni condivise con soggetti esterni e delle persone o entità coinvolte. Questo può aiutare a monitorare la diffusione delle informazioni e ad individuare eventuali violazioni della sicurezza.

7.8. Formazione e Consapevolezza sulla Sicurezza Informatica

Tutti i dipendenti dell'azienda sono tenuti a partecipare a programmi di formazione sulla sicurezza informatica. Questi programmi includono le buone prassi nell'uso dei sistemi informatici, le politiche di sicurezza da rispettare, le tecniche di protezione dei dati e la prevenzione delle minacce informatiche. La formazione sulla sicurezza informatica è parte integrante delle responsabilità di ogni dipendente, indipendentemente dal ruolo o dal livello di esperienza.

7.9. Violazioni delle Politiche di Sicurezza

Le violazioni delle politiche di sicurezza devono essere immediatamente segnalate al Responsabile per la gestione dei sistemi informatici aziendali. Questo include qualsiasi sospetto di accesso non autorizzato, uso improprio delle risorse informatiche, perdita di dati o altre violazioni della sicurezza. Le violazioni delle politiche di sicurezza possono comportare azioni disciplinari, fino al licenziamento.

7.10. Revisione e Aggiornamento delle Politiche di Sicurezza

Le politiche di sicurezza devono essere regolarmente riviste e aggiornate per rispondere alle mutevoli esigenze dell'azienda, all'evoluzione della tecnologia e alle nuove minacce alla sicurezza informatica. Tutti i dipendenti devono essere aggiornati sulle modifiche apportate alle politiche di sicurezza e devono adeguare il proprio comportamento di conseguenza

7.11. Aggiornamenti e procedure di patch

Tutte le patch di sicurezza ritenute rilevanti devono essere testate in un ambiente controllato prima dell'implementazione. Le patch di sicurezza critiche devono essere implementate il più rapidamente possibile, in linea con le procedure interne. Il software deve essere mantenuto alla versione più recente supportata dal fornitore, a meno che non ci siano ragioni valide per non farlo.
Gli aggiornamenti del software devono essere pianificati e implementati in modo da minimizzare l'impatto sulle operazioni aziendali. Tutti i sistemi devono essere mantenuti in conformità con le leggi, i regolamenti e le normative applicabili. Il dipartimento IT può condurre regolari audit di conformità per assicurarsi che tutti i sistemi siano aggiornati e patchati. Le violazioni di questa policy possono comportare azioni disciplinari, fino al licenziamento.

8. Uso della posta elettronica

8.1. La casella di posta elettronica, anche se assegnata specificamente all'utente indicando in tutto o in parte nell'indirizzo il suo cognome e/o nome, è uno strumento di lavoro. L'uso per motivi personali deve essere moderato ed è tollerato esclusivamente ai sensi dell'articolo seguente. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

8.2. La Società è consapevole della possibilità di un limitato utilizzo personale della posta elettronica da parte degli incaricati e allo scopo prevede le seguenti misure:
- in caso di ricezione sulla e-mail aziendale di posta personale si avverte di cancellare immediatamente ogni messaggio al fine di evitare ogni eventuale e possibile back up dei dati;
- avvisare la Società quando alla propria casella di posta aziendale siano allegati files eseguibili e/o di natura incomprensibile o non conosciuta.

8.3. L'accesso alla posta elettronica è personale e avviene tramite nome utente e password. È fatto divieto di utilizzare le caselle di posta elettronica per motivi diversi da quelli strettamente legati all'attività lavorativa fatto salvo quanto indicato al precedente paragrafi 8.1 e 8.2. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:
- 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 (o di Sant'Antonio). Se si riceveranno peraltro messaggi di tale tipo, si dovrà comunicarlo immediatamente al personale designato dalla Società. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

8.4. La casella di posta deve essere mantenuta in ordine, archiviando o cancellando documenti inutili e soprattutto allegati ingombranti. Si ricorda che a fronte dell'attività di formattazione del Personal Computer, personale designato dalla Società può provvedere al backup dell'archivio di posta.

8.5. È obbligatorio porre la massima attenzione nell'aprire i file allegati di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

8.6. Al fine di garantire la funzionalità del servizio di posta elettronica aziendale e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, il sistema, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella) invierà automaticamente messaggi di risposta contenenti le "coordinate" di posta elettronica di un altro soggetto o altre utili modalità di contatto della struttura. In tal caso, la funzionalità deve essere attivata dall'utente o se in difficoltà dal personale designato dalla Società.

8.7. In caso di assenza non programmata (ad es. per malattia) la procedura - qualora non possa essere attivata dal lavoratore a distanza entro due giorni - verrà attivata a cura della Società.

8.8. Informato l'utente e anche per interposta persona indicata dall'utente, la Società potrà accedere, alla casella di posta elettronica dell'utente medesimo per ogni ipotesi in cui ciò si renda necessario, sempre nel più assoluto rispetto delle prescrizioni indicate nelle Linee guida del Garante Privacy per posta elettronica e internet del 1° marzo 2007, in caso di utilizzo di personal computer e device aziendali.

8.9. Il personale designato dalla Società, nell'impossibilità di procedere come sopra indicato e nella necessità di non pregiudicare la necessaria tempestività ed efficacia dell'intervento, potrà, informato l'utente, accedere alla casella di posta elettronica per le sole finalità indicate al punto 3.4, sempre nel più assoluto rispetto delle prescrizioni indicate nelle Linee guida del Garante Privacy per posta elettronica e internet del 1° marzo 2007, in caso di utilizzo di personal computer e device aziendali.

8.10. A seguito della cessazione del rapporto lavorativo e/o professionale dell'utente con la Società, quest'ultima procederà alla chiusura della relativa e-mail aziendale e attiverà un sistema di risponditore automatico con indicazione di un indirizzo alternativo a cui inviare la comunicazione. La Società procederà altresì alla cancellazione della casella di posta appartenente all'utente decorso un periodo di 3-6 mesi (a discrezione, in base al ruolo aziendale) dalla cessazione del rapporto lavorativo e/o professionale, fatto salvo un eventuale interesse legittimo specifico della Società che legittimi concretamente la conservazione della posta per un periodo superiore (es. azione giudiziale minacciata o pendente).

8.11. Al fine di ribadire agli interlocutori la natura esclusivamente aziendale della casella di posta elettronica, i messaggi devono contenere un avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi precisando che, pertanto, il personale debitamente designato della Società potrà accedere al contenuto del messaggio inviato alla stessa casella secondo le regole fissate nella propria policy aziendale.

9. Navigazione in Internet

9.1. Il device assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa, anche fuori dall'orario di lavoro. L'utilizzo per scopi personali è permesso con moderazione e con gli accorgimenti di cui al presente documento.

9.2. La Società potrà adottare idonee misure tecniche preventive volte a ridurre navigazioni a siti non correlati all'attività lavorativa attraverso filtri e black list.

9.3. A titolo puramente esemplificativo, l'utente non potrà utilizzare Internet per:

- l'upload o il download di software gratuiti (freeware) e shareware;
- l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (per es. filmati o file musicali) e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà venir a tal fine contattato il personale designato dalla Società);
- l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dai preposti aziendali e comunque nel rispetto delle normali procedure di acquisto;
- 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 nickname) se non espressamente autorizzati dalla Società
- la navigazione è sempre vietata nei siti che possono rivelare le opinioni politiche religiose, sindacali, di salute e/o qualsiasi informazione che possa rivelare dati sensibili o di natura particolare dell'utente;
- accedere a siti internet che abbiano un contenuto contrario a norme di legge e a norme a tutela dell'ordine pubblico, rilevante ai fini della realizzazione di una fattispecie di reato o che siano in qualche modo discriminatori sulla base della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap.

9.4. Gli eventuali controlli relativi alla navigazione in Internet, compiuti dal personale designato dalla Società, potranno avvenire mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta, identificando gli utenti su base collettiva o per gruppi sufficientemente ampi di lavoratori. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'azienda, sulla base di principi di correttezza e necessità previsti dalla legge in materia di privacy.

9.5. I L'uso dei social network è consentito in modalità personale per scopi non lavorativi, al di fuori dell'orario di lavoro e mediante sistemi e credenziali non aziendali. Tuttavia, per quelle figure che, nell'ambito della loro funzione (ad es. social media manager) o per i colleghi che devono interagire con tali piattaforme a supporto delle attività aziendali, l'utilizzo dei social network risulta necessario, è consentito l'accesso mediante account personali o dedicati, sempre nel rispetto delle seguenti condizioni:
Non devono essere divulgate informazioni riservate o confidenziali;
Le comunicazioni devono essere conformi alle linee guida aziendali, al fine di tutelare l'immagine e la reputazione della Società;
Le opinioni espresse devono essere chiaramente identificate come personali, salvo espressa autorizzazione a rappresentare la posizione ufficiale della Società.
In ogni caso, è vietato utilizzare credenziali aziendali e strumenti aziendali (es. email) per l'accesso ai social network, ma essi vanno gestiti nelle modalità e best practise previste dagli stessi.

9.6. L'accesso alla rete WiFi aziendale è riservato solo per scopi lavorativi. Le credenziali di accesso non devono essere condivise con persone esterne all'organizzazione. Qualora sia necessario mettere a disposizione di visitatori e/o ospiti un punto di accesso a Internet è obbligatorio fornire a questi ultimi le credenziali del la rete WiFi di tipo guest dedicata agli ospiti, rimanendo espressamente consentire a questi ultimi l'accesso e l'utilizzo della rete aziendale. Le altre reti sono ad uso esclusivo interno. L'uso della rete WiFi non deve in alcun modo violare le leggi o i regolamenti applicabili. Non è consentito l'accesso a siti web illegali, offensivi o inappropriati. Non è consentito l'uso della rete WiFi per scaricare o trasmettere materiale protetto da copyright senza l'autorizzazione appropriata.
I dispositivi che accedono alla rete WiFi devono avere software antivirus aggiornati e patch di sicurezza. Non è consentito l'uso di VPN personali o di altri strumenti che bypassano le misure di sicurezza della rete. Qualsiasi sospetto di violazione della sicurezza deve essere immediatamente segnalato al dipartimento IT. Le violazioni di questa policy possono comportare l'accesso limitato o negato alla rete WiFi e altre possibili azioni disciplinari, fino al licenziamento.

10. Protezione antivirus

10.1. Il sistema informatico della Società è protetto da software antivirus aggiornato continuativamente. 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.

10.2. Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l'accaduto al personale designato dalla Società.

10.3. Ogni dispositivo elettronico di provenienza esterna alla Società dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale designato dalla Società.

10.4. E' severamente vietato tentare di manomettere l'antivirus e/o di disinstallarlo senza previa autorizzazione in casi eccezionali del responsabile IT.

11. Utilizzo dei telefoni e fotocopiatrici aziendali

11.1. 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 a carattere personale o comunque non strettamente inerenti all'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali è consentita solo nel caso di comprovata necessità ed urgenza.

11.2. Qualora venisse assegnato un cellulare aziendale all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Al cellulare aziendale si applicano le medesime regole sopra previste per l'utilizzo del telefono aziendale: in particolare è vietato l'utilizzo del telefono cellulare messo a disposizione per inviare o ricevere SMS o MMS o altra tipologia di messaggi anche tramite applicazioni, di natura personale o comunque non pertinenti lo svolgimento dell'attività lavorativa. L'eventuale uso promiscuo (anche per fini personali) del telefono cellulare aziendale è possibile soltanto in presenza di preventiva autorizzazione scritta e in conformità delle istruzioni al riguardo impartite dal personale designato dalla Società.

11.3. È vietato l'utilizzo delle fotocopiatrici aziendali per fini personali, salvo preventiva ed esplicita autorizzazione da parte della Società.

12. Osservanza delle disposizioni in materia di Privacy

12.1. È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure di sicurezza adeguate di cui agli artt. 5 e segg. e 32 e segg. del Regolamento Privacy, come indicato nella lettera di designazione ad incaricato del trattamento, e ai provvedimenti dell'Autorità Garante della protezione dei dati personali in quanto applicabili, come adottate dalla Società nel presente Regolamento e/o in altre disposizioni e/o procedure aziendali.

13. Accesso ai dati trattati dall'utente

13.1. 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, ecc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà della Società, tramite il personale appositamente designato o addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.

14. Sistemi di controlli graduali

14.1. Nel più assoluto rispetto delle prescrizioni indicate nelle Linee guida del Garante Privacy per posta elettronica e internet del 1° marzo 2007, in caso di utilizzo di personal computer e device aziendali, in caso di anomalie, il personale designato dalla Società effettuerà controlli anonimi che si concluderanno con avvisi generalizzati diretti ai dipendenti dell'area o del settore in cui è 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 computi solo in caso di successive ulteriori anomalie e, con riferimento ai dipendenti, ad istanza della direzione del personale. In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

15. Gestione dati cartacei

15.1. Gli utenti sono responsabili del controllo e della custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.

15.2. Gli utenti sono invitati ad adottare una "politica della scrivania pulita". Ovvero si richiede agli utenti di trattare dati cartacei solo se necessario, privilegiando, ove possibile, l'utilizzo degli strumenti digitali messi a disposizione dalla Società. I principali benefici di una politica della scrivania pulita sono:

- una buona impressione a clienti e fornitori che visitano la nostra organizzazione;
- la riduzione della possibilità che informazioni confidenziali possano essere viste da persone non abilitate a conoscerle;
- a riduzione che documenti confidenziali possano essere sottratti all'organizzazione.

In particolare, con riferimento ai dipendenti:

- si invita a non lasciare in vista sulla propria scrivania dati cartacei quando ci si allontana dalla stessa oppure quando è previsto un incontro con un soggetto non abilitato alla conoscenza dei dati in essi contenuti;
- prima di lasciare la propria postazione (per esempio per la pausa pranzo o per una riunione) sarà cura degli Incaricati riporre in luogo sicuro (armadio, cassettiera, archivio, ecc.) i dati cartacei ad esso affidati, affinché gli stessi non possano essere visti da terzi non autorizzati (es. addetti alle pulizie) o da terzi (visitatori) presenti nell'organizzazione;
- a fine giornata deve essere previsto il riordino della scrivania e la corretta archiviazione di tutte le pratiche d'ufficio, in modo da lasciare la scrivania completamente sgombra;
- è necessario rimuovere immediatamente ogni foglio stampato da una stampante o da un'apparecchiatura fax, per evitare che siano prelevati o visionati da soggetti non autorizzati.

15.3. Ove possibile, si invita ad evitare la stampa di documenti digitali, anche ai fini di ridurre l'inquinamento ed il consumo delle risorse in ottica ecologica. Ove possibile, si invita ad effettuare la scansione dei documenti cartacei ed archiviarli digitalmente.

16. Profili autorizzativi

16.1. Per Profilo Autorizzativo (o privilegio utente), si intende un insieme di regole, relativo ad un applicazione/servizio, che ne definiscono le modalità di utilizzo da parte degli Utenti. Queste regole possono essere espresse nell'insieme di risorse ed attributi (c.d ruoli applicativi - Amministratore, Utente, Operatore) che ne regolano l'accesso.
I profili autorizzativi devono essere:

- definiti sulla base delle specifiche applicazioni informatiche (es. sistemi, apparati di rete) che gli utenti devono utilizzare durante la normale attività lavorativa;
- in ragione del ruolo ricoperto e limitatamente alle mansioni svolte;
- configurati per limitare l'accesso ai soli dati necessari alle finalità dell'attività lavorativa (principi del "at least privilege" e "need to know")
- limitate nel tempo in ragione delle effettive necessità lavorative.

16.2. I Responsabili dei vari uffici hanno facoltà di richiedere, per i propri collaboratori, l'accesso agli applicativi in uso stabilendo preventivamente i profili autorizzativi strettamente necessari alle funzioni per cui sono incaricati (compatibilmente al livello di responsabilità e al contesto in cui operano). La richiesta deve essere formulata all'Ufficio IT che provvede, a seconda dei casi, all'abilitazione all'accesso e/o alla modifica dei profili di autorizzazione.

17. Sanzioni

17.1. Il mancato rispetto o la violazione delle regole contenute nella Policy, è perseguibile con provvedimenti disciplinari commisurati alla violazione, nonché con le azioni civili e penali previste dalla normativa vigente. Si precisa che l'applicazione delle sanzioni disciplinari prescinde dall'esito di un eventuale procedimento penale, in quanto le regole imposte dalla Policy sono assunte dalla Società in piena autonomia e indipendentemente dalla tipologia di illecito che singole violazioni possono determinare. La Società si riserva inoltre di agire a propria tutela per ottenere il risarcimento di danni eventualmente provocati dall'utente che ha generato comportamenti non corretti, ha agito con incuria e/o ha agito con manifesta volontà di ledere la Società.

18. Aggiornamento e revisione

18.1. Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente Regolamento. Le proposte verranno esaminate dalla Società.

18.2. Il presente Regolamento è soggetto a revisione ogni qualvolta intervengano modifiche inerenti alle disposizioni elencate e, in ogni caso, quando ritenuto opportuno dalla Società.

Data **Firma**

_____ _____