REGOLAMENTO INTERNO – INTERNET ed EMAIL

Stesura	Data	Firma
Redatto da: Daniele Peressutti	25/05/18	
Verificato da: Elio Pantanali	25/05/18	
Approvato da: Elio Pantanali	25/05/18	

Rev. n°	Oggetto della revisione	Data
1.0	Prima Emissione	25/05/18
2.0	Revisione Annuale	31/03/19
3.0	Revisione Annuale	31/03/20

Distribuzione	Originale presso
GENERALE	Responsabile Direzione SI

INDICE

Introduzione

I sistemi informativi rivestono ormai un ruolo fondamentale all'interno dei processi produttivi di un'azienda.
Vista la diffusione delle nuove tecnologie informatiche e l'utilizzo non appropriato di strumenti quali Internet e posta elettronica, si espone l'azienda ai rischi di un coinvolgimento sia di carattere patrimoniale che penale, creando inoltre problemi alla sicurezza e all'immagine dell'Azienda stessa.

I punti fondamentali per garantire la sicurezza si possono riassumere in :

- **Integrità e consistenza** : informazioni corrette e complete;
- **Disponibilità** : accessibilità ai dati ed alle risorse quando questi servono realmente;
- **Riservatezza** : l'accesso ai dati deve essere limitato solamente alle persone per cui è previsto;
- **Conformità** : rispetto delle normative vigenti.

Le caratteristiche relative alle misure di sicurezza, possono essere desunte analizzando la provenienza delle potenziali minacce informatiche.
I rischi più frequenti a cui si può andare incontro, possono essere classificati in 5 categorie :

- Guasti hardware;
- Errori dei software;
- Intrusioni dall'esterno;
- Errori nelle procedure del personale tecnico;
- **Comportamento degli utenti interni ed esterni, Agenti ed eventuali fornitori che abbiamo accesso al sistema informativo aziendale ed ai dati contenuti in esso**.

È molto importante considerare le minacce provenienti dai comportamenti degli utenti del sistema informatico, che spesso si originano da una insufficiente comprensione delle conseguenze delle proprie azioni o da un mancato rispetto delle procedure.

I rischi possono essere generati, ad esempio :

- Navigando all'interno di "siti pericolosi";
- Utilizzando credenziali di autenticazione in modo non riservato;
- Salvando i documenti in archivi non protetti (rischio di perdita di dati);
- Scaricando file non autorizzati o non necessari da Internet (rischio virus, saturazione banda, saturazione archivi).

Per limitare i rischi ai sistemi informativi aziendali, è necessario rendere consapevoli gli utenti riguardo i danni che potrebbero essere generati da comportamenti non corretti ed indicare le procedure da seguire.

È fondamentale, quindi, redarre un regolamento interno come il seguente e la relativa opera di formazione del personale. Questi sono i principali motivi del perché viene istituito questo documento, in stretta relazione al fatto che serve da linea guida agli utilizzatori degli strumenti informatici aziendali per evitare di incorrere in sanzioni che (come previsto dalla legge 196/03 e successive modifiche e del Regolamento UE n. 2016/679) può arrivare fino a risvolti penali.

Il regolamento, quindi, non deve essere considerato come uno strumento impositivo, ma come una guida ai corretti comportamenti e viene utilizzato per la preparazione e motivazione degli utenti.

La funzione del regolamento è comunque di carattere sanzionatorio, qualora vengano riscontrati comportamenti scorretti. Valgono quindi tutte le modalità previste per la validità disciplinare di un regolamento aziendale.

I principi del regolamento possono essere riassunti in questi punti :

- Il computer è uno strumento di lavoro, affidato all'utente;
- L'utente non è di norma abilitato a modificare la struttura hw/sw del computer;
- L'utente è tenuto al rispetto delle normative vigenti, elencate nel seguito;
- Devono essere seguite le procedure di gestione della sicurezza previste.

Rispetto delle normative

Normative fondamentali

- Regolamento UE n. 2016/679;
- Legge sulla privacy (D.Lgs. 30 Giugno 2003, n. 196/03);
- Provvedimento Generale del 1° Marzo 2007 (Linee guida per posta elettronica ed internet);
- Normativa sul diritto d'autore (vari provvedimenti fino al Decreto Legislativo 16 marzo 2006, n. 140);
- Codice penale : sezione reati informatici.

Normativa sul diritto d'autore

- Tutto il software utilizzato in azienda deve essere dotato di regolare licenza;
- L'Azienda provvede all'installazione di tutto il software presente in un computer;
- Le violazioni sono sanzionate anche penalmente.

Codice Penale

- Utilizzo illecito di credenziali di autenticazione;
- Intrusione in sistemi informatici;
- Distruzione o manipolazione di informazioni o sistemi informatici;
- Utilizzo dei sistemi come "zombies" per lo svolgimento di attività illecite;
- La configurazione di un sistema dotato di adeguate misure di protezione può permettere all'azienda di far valere i propri diritti in sede giudiziaria e ridurre la responsabilità verso terzi.

Possibilità e modalità di controllo

Sintetizzando il provvedimento del 1° marzo 2007 (linee guida del garante sull'utilizzo di email e Internet sui luoghi di lavoro) si può dire che :

- Non è autorizzato un sistema di controllo sistematico, preventivo e generalizzato;
- Non sono autorizzati i controlli occulti;
- Sono da privilegiare i sistemi che impediscono ex ante le attività non autorizzate, rendendo quindi non necessari i relativi controlli ex post;
- I controlli devono essere configurati in modo da permettere un dettaglio sempre maggiore, mediante approfondimento, SOLO in caso di necessità;
- Gli utenti devono essere informati sui sistemi di controllo esistenti.

Per rendere normativamente valide le modalità di controllo qui descritte, devo essere garantiti i seguenti presupposti :

- Esistenza di un regolamento informatico che escluda la possibilità di utilizzo personale dei sistemi informatici;
- Informativa ai dipendenti sui sistemi di controllo esistenti (contenuta nel Regolamento);
- Rispetto della normativa privacy.

Posta elettronica

I messaggi di posta elettronica hanno un rilevante valore aziendale.
L'accesso ai messaggi di posta elettronica deve essere possibile anche in assenza del mittente/destinatario, come per qualsiasi comunicazione o documentazione aziendale.

Navigazione

È necessario effettuare un controllo sul servizio di navigazione per prevenire un utilizzo di banda anomalo e garantire che il servizio venga utilizzato per gli scopi prefissati (analisi dei siti visitati in forma anonima).
L'accesso ad internet è limitato alle persone che lo necessitano e solo per i servizi previsti, ad eccezione di una fascia oraria coincidente con la pausa pranzo in cui l'accesso è libero.

Regolamento Aziendale per l'utilizzo delle risorse informatiche e di rete

Viste le premesse descritte nell'introduzione, si rende necessario attivare una serie di norme, restrizioni e controlli per garantire la sicurezza dei sistemi informativi e definire le responsabilità degli utilizzatori delle risorse e degli amministratori di sistema.

I Sistemi Informativi Aziendali hanno la responsabilità della configurazione e dell'amministrazione delle risorse informatiche e delle reti.

Per risorse informatiche si intendono :

- dispositivi dei Sistemi Informativi (installati presso il data center);
- workstation, personal computer, notebook, smartphone, cellulari e stampanti utilizzati da dipendenti, amministratori, personale con incarichi professionali, stagisti ed eventuali ospiti;
- apparati di rete;
- tutto il software ed i dati acquistati, prodotti o trattati per l'amministrazione dei sistemi e per l'utilizzo da parte degli utenti o di terzi autorizzati.

Regolamento interno per l'utilizzo della rete aziendale e dei servizi Internet e posta elettronica

Le seguenti regole devono essere seguite scrupolosamente da tutti gli utilizzatori della Rete aziendale e cioè : dipendenti, amministratori, personale con incarichi professionali, stagisti ed eventuali ospiti debitamente autorizzati.

In caso di dubbi o necessità di chiarimenti su come comportarsi in situazioni particolari, è opportuno contattare l'Amministratore di sistema.

Per quanto non specificato nel presente documento, è richiesto comunque un atteggiamento ispirato alla correttezza ed alla buona fede ed in qualunque caso l'utilizzatore riesca a compiere azioni dubbie o che non dovrebbero essere permesse, segnalare immediatamente alle persone preposte questi incidenti sulla sicurezza.
Inoltre, per tutto quanto non sia controllabile e quindi non riportato in questo documento, le eventuali conseguenze dei problemi che ne possono uscire ricadranno sempre e comunque sul singolo utilizzatore.

Resta valida, in ogni caso, l'assunzione di responsabilità personale per i dispositivi e gli strumenti dati in uso dall'Azienda.

1. Utilizzo delle risorse informatiche aziendali

1.1 Le risorse informatiche affidate al dipendente sono strumenti di lavoro. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e soprattutto, minacce alla sicurezza. Il mancato rispetto di tale regola potrà comportare l'avvio di un procedimento disciplinare a cura dell'Ufficio Personale in base a quanto disposto dal vigente CCNL di settore.
1.2 L'accesso alle risorse informatiche viene protetto con password che deve essere custodita dall'utente con la massima diligenza e non divulgata. La stessa password potrà essere attivata, secondo quanto stabilito dall'Amministratore di Sistema, per l'accesso a qualsiasi applicazione, dato o strumento, per lo screen saver e per il collegamento alla rete Internet.
1.3 L'amministratore di sistema al solo fine di espletare le sue funzioni, ha la facoltà di accedere (informando preventivamente l'interessato), in qualsiasi momento, alle applicazioni ed ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica interna ed esterna. In caso di assenza improvvisa o prolungata e per improrogabili necessità legate alle attività lavorative, l'Amministratore di sistema, potrà accedere agli archivi di ogni utente anche senza il consenso preventivo dell'interessato, che sarà informato tempestivamente dell'intervento.
1.4 Non è consentito installare autonomamente nessun tipo di programma salvo preventiva ed esplicita autorizzazione dell'Amministratore di sistema. In caso di necessità di acquisto o di dotazione di software applicativi e/o procedure pertinenti esclusivamente alcune aree ed i relativi dirigenti, deve essere comunque richiesta l'autorizzazione preventiva da parte dell'Amministratore di sistema, per poter garantire la compatibilità funzionale, tecnica ed il mantenimento dell'efficienza operativa dei sistemi e delle reti. Ciò in quanto sussiste il grave pericolo di introdurre virus informatici, di alterare la stabilità delle applicazioni installate sulle risorse informatiche o di compromettere la consistenza della base dati aziendale.
1.5 E' assolutamente vietato l'uso di programmi diversi da quelli distribuiti ufficialmente dall'azienda (dlg. 518/92 sulla tutela giuridica del software e l. 248/2000 "Nuove norme di tutela del diritto d'autore").
1.6 Salvo giustificate necessità legate allo svolgimento delle mansioni assegnate, non è consentito all'utente di modificare le caratteristiche impostate sul proprio PC. Ogni modifica può essere effettuata solamente da parte dell'Amministratore di sistema.
1.7 Personal computer e notebook devono essere spenti ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In ogni caso è obbligatorio mantenere protette le proprie risorse informatiche tramite screen saver con password, per evitare accessi di terzi, senza che vi sia la possibilità di provarne in seguito l'indebito uso.
1.8 Non è consentita l'installazione di alcun dispositivo o periferica di memorizzazione, comunicazione o altro non distribuito dai Sistemi Informativi (ad es. masterizzatori, chiavette USB non aziendali, etc.) ovvero senza l'autorizzazione dell'Amministratore di sistema.
1.9 Agli utenti incaricati del trattamento dei dati sensibili è fatto divieto di accedere contemporaneamente con lo stesso account da più PC.

1.10 Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, segnalando tempestivamente all'Amministratore di sistema ogni tipo di malfunzionamento o eventuale virus ed adottando quanto previsto dal successivo punto 9.3 del presente Regolamento.
1.11 Non è consentita la creazione e memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza politica e/o sindacale o che comunque configurino ipotesi di reato secondo le vigenti leggi.

2. Utilizzo della rete informatica aziendale (uso delle cartelle di scambio)

2.1 Le unità di rete sono aree pubbliche di condivisione di informazioni strettamente professionali e non possono essere in alcun modo utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, verranno svolte regolari attività di controllo a cadenza mensile e di amministrazione e backup a cadenza giornaliera da parte dell'Amministratore di sistema.
2.2 Le password d'ingresso alla rete e a tutti gli applicativi aziendali, sono segrete e vanno comunicate e gestite secondo le procedure impartite (fare riferimento al punto 3 del seguente regolamento). È assolutamente vietato accedere alla rete ed ai programmi con nomi utente diversi dal proprio.
2.3 L'Amministratore di sistema può, in qualunque momento, procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosa per la sicurezza sia dei PC che delle unità di rete.
2.4 Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti od inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati ed alle email. È infatti da evitare un'archiviazione dei dati ridondante. Il Servizio Sistemi Informativi si riserva inoltre di effettuare controlli con una cadenza mensile per determinare eventuali anomalie nell'utilizzo dello spazio disco utilizzato.
2.5 Tutti i file presenti nelle cartelle di rete, sono sottoposti a backup giornaliero incrementale. È possibile ripristinare i file eventualmente eliminati, fino a quattro versioni precedenti all'ultima disponibile.
2.6 È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. È buona norma evitare di stampare documenti o file lunghi e complessi su stampanti comuni. Preferire le stampanti laser per questa tipologia di stampe, cercando di concentrare i lavori in orari tali da non rallentare il loro normale utilizzo. In caso di necessità la stampa in corso potrà essere cancellata. Verranno inoltre distribuiti ai responsabili di ogni ufficio, report periodici con dati aggregati relativi all'utilizzo delle stampanti.

3. Gestione delle password

3.1 Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite dall'Amministratore di sistema per consentire un primo accesso ai sistemi aziendali. In seguito, l'utente dovrà modificare la sua password seguendo le indicazioni riportate al punto 3.2 di questo regolamento.
3.2 Le password devono essere lunghe almeno otto caratteri, (salvo limitazioni di particolari applicazioni) formate da lettere (maiuscole e/o minuscole), numeri e caratteri speciali quali & % ^ # $, ricordando che lettere maiuscole e minuscole hanno significati diversi per i sistemi, evitando ovviamente contenuti di senso logico immediato che sono facilmente individuabili (esempio : date di nascita, nome e cognome, etc.).
3.3 Le password utilizzate dagli incaricati al trattamento hanno una durata massima di 2 mesi, trascorsi i quali, le password devono essere sostituite.
3.4 La password deve essere immediatamente sostituita nel caso si sospetti che la stessa abbia perso la segretezza.
3.5 Qualora l'utente venisse a conoscenza delle password di un altro utente, è tenuto a darne immediata notizia al proprio responsabile ed in seconda battuta anche all'Amministratore di Sistema per la sua immediata sostituzione.
3.6 Sarà cura dei Dirigenti e dei Responsabili di sezione, comunicare tempestivamente eventuali cambi di mansione che comportino modifiche o revoche di autorizzazione all'accesso delle risorse informatiche, sia all'ufficio del personale che all'Amministratore di Sistema, per iscritto, al fine di rendere possibili le modifiche ai profili di accesso alle risorse e la sostituzione delle password ove necessario. Verranno inoltre forniti report periodici contenenti la situazione dei profili, per consentire un loro rapido controllo.

4. Utilizzo dei supporti di memorizzazione

4.1 Tutti i supporti magnetici riutilizzabili (hard disk esterni, memorie USB, ecc...), il cui utilizzo è autorizzato preventivamente dall'Amministratore di sistema e contenenti dati aziendali, devono essere trattati con particolare cautela, onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe essere in grado di recuperare i dati memorizzati anche dopo la loro cancellazione.
4.2 I supporti magnetici contenenti dati sensibili devono essere custoditi in archivi chiusi a chiave.
4.3 Non è consentito scaricare ed eventualmente memorizzare files e dati, non aventi alcuna attinenza con la propria prestazione lavorativa, su supporti magnetici e/o ottici.

5. Utilizzo delle risorse informatiche portatili

5.1 L'utente è responsabile dei dispositivi portatili assegnatogli dall'Amministratore di sistema e deve custodirli con diligenza, sia durante gli spostamenti, sia durante l'utilizzo nel luogo di lavoro.
5.2 Ai dispositivi portatili si applicano le regole previste per le altre risorse informatiche connesse in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.
5.3 I dispositivi portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi in un luogo protetto.
In caso di furto o sottrazione, oltre alle necessarie denunce alle Autorità, deve essere fatta comunicazione immediata all'Amministratore di sistema, per consentire la disattivazione di tutti i collegamenti remoti alla rete aziendale.
5.4 Eventuali configurazioni particolari quali connessioni di acceso remoto, connessioni RDP, collegamenti VPN, collegamenti di periferiche personali (smartphone, chiavi USB, ecc…), dirette verso la rete aziendale o attraverso Internet, devono essere autorizzate esclusivamente a cura dell'Amministratore di sistema e del suo staff tecnico. Verranno inoltre prodotti report periodici relativi all'utilizzo delle connessioni remote (il traffico generato dai collegamenti remoti è riconducibile al proprietario; il traffico viene costantemente monitorato in termini di quantità di dati scambiati tra server e client connesso).

6. Utilizzo della posta elettronica

6.1 La casella di posta elettronica, assegnata dall'Azienda a ciascun utente, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
6.2 È importante segnalare che è prevista una procedura automatica di backup dei messaggi di posta elettronica ed eventuali allegati a cadenza giornaliera.
6.3 È fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum, mailing list non attinenti alla propria mansione e comunque non autorizzati dal Responsabile.
6.4 È buona norma evitare messaggi estranei al rapporto di lavoro od alle relazioni professionali fra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto ingombranti.
6.5 Prestando attenzione alla dimensione degli allegati, (la dimensione massima è fissata in 10 MB in ricezione ed in spedizione) è possibile utilizzare la posta elettronica per la trasmissione di files all'interno dell'Azienda. Qualora il file non abbia un contenuto riservato è preferibile utilizzare l'apposita cartella "scambio" che si trova sul file server di rete.
6.6 È obbligatorio controllare i file attachments di posta elettronica prima del loro utilizzo ed è vietato eseguire download di file eseguibili o documenti da siti web o ftp non attendibili.

6.7 È vietato iniziare o proseguire catene telematiche (o di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo è obbligatorio darne immediata comunicazione all'Amministratore di sistema. Gli eventuali allegati di tali messaggi non devono in alcun modo essere eseguiti.
6.8 In previsione della possibilità che, in assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica di un utente, l'Amministratore di sistema potrà verificare il contenuto di messaggi ed inoltrare al titolare del trattamento, quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. A cura del titolare del trattamento, di tale attività, verrà redatto apposito verbale ed informato il lavoratore interessato alla prima occasione utile.

7. Uso della rete internet e relativi servizi

7.1 Il servizio di navigazione Internet viene abilitato, agli utenti che ne fanno richiesta, esclusivamente per esigenze lavorative e previa richiesta del relativo Responsabile di sezione. Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. È proibita la navigazione in Internet per motivi diversi da quelli funzionali all'attività lavorativa stessa.
7.2 È fatto divieto all'utente il download di qualsiasi tipo di software prelevato da Internet, se non espressamente autorizzato dall'Amministratore di sistema.
7.3 È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on line e simili, salvo i casi direttamente autorizzati o attinenti i compiti e le mansioni assegnate e con il rispetto delle normali procedure di acquisto.
7.4 È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
7.5 È vietata la partecipazione a forum non professionali, l'utilizzo di chat-line (esclusi gli strumenti autorizzati), di bacheche o blog, registrazioni in guest books anche utilizzando pseudonimi (o nicknames), se non attinenti l'attività lavorativa svolta e previa autorizzazione del responsabile.
7.6 Non è consentita la navigazione in siti ove sia possibile rivelare le opinioni politiche, religiose o sindacali dell'utilizzatore; non è consentito inoltre visitare siti e memorizzare documenti informatici dai contenuti di natura oltraggiosa e/o discriminatoria per sesso/etnia/religione/opinione e/o appartenenza sindacale e/o politica.
7.7 Il Servizio Sistemi Informativi si riserva di applicare per singoli o gruppi di utenti, politiche di navigazione personalizzate in base alle mansioni ed eventuali disposizioni concordate con la Direzione e con i Responsabili di sezione, al fine di ottimizzare l'uso delle risorse, gli investimenti e le prestazioni delle connessioni esistenti.
7.8 È da ritenersi vietata, ogni altra attività illegale secondo le vigenti norme, qui non elencata.

8. Sistemi di controllo remoto

8.1 L'Amministratore di sistema ed i suoi collaboratori, ai soli fini di assistenza tecnica (help desk), possono procedere al collegamento remoto verso le postazioni degli utenti che necessitino di un intervento, previo consenso dell'utente interessato.
8.2 L'Amministratore di sistema si riserva, nel caso di situazioni di emergenza, di effettuare il collegamento remoto ad una postazione di lavoro, anche senza il consenso della persona interessata, riservandosi di informare l'utente dell'intervento eseguito alla prima occasione utile.

9. Protezione Antivirus

9.1 Ogni utente è tenuto a controllare il regolare funzionamento e l'aggiornamento periodico del software antivirus installato.
9.2 Nel caso il software antivirus rilevi la presenza di virus o altre minacce informatiche, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer e segnalare l'accaduto all'Amministratore di sistema.
9.3 Non è consentito l'utilizzo di pen drive, cd o dvd rom, cd o dvd riscrivibili ed altri supporti magnetici od ottici di provenienza ignota.
9.4 Ogni dispositivo magnetico o ottico di provenienza esterna all'azienda dovrà essere verificato mediante programma Antivirus prima del suo utilizzo e nel caso venga rilevato un virus, dovrà essere consegnato all'Amministratore di sistema.

10. Utilizzo delle utenze telefoniche

10.1 Al pari delle risorse informatiche, le utenze telefoniche aziendali assegnate (siano esse fisse o mobili) costituiscono beni aziendali e specifici strumenti di lavoro. Ne deriva che l'utilizzo delle stesse per scopi privati (o comunque estranei all'attività lavorativa), deve considerarsi vietato. Il Servizio Sistemi Informativi si riserva inoltre di effettuare controlli a carattere generale (come previsto dal punto 6.1 del Provvedimento del Garante) per determinare eventuali anomalie nell'utilizzo del servizio telefonico.
10.2 Si ricorda che ogni utilizzo degli apparati telefonici per scopi non aziendali non è consentito.
10.3 I Sistemi Informativi a cadenza trimestrale eseguiranno dei controlli a livello di ufficio sul corretto uso degli strumenti telefonici.

Osservanza delle disposizioni in materia di Privacy

E' obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza. Tale norma è indicata nelle lettere di nomina dell'incaricato al trattamento dei dati ai sensi del D.lgs 196/03 e del Regolamento UE n. 2016/679.

Non osservanza della normativa aziendale

Il presente documento costituisce "REGOLAMENTO AZIENDALE".
Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite (previste sempre dal CCNL vigente).

Aggiornamento e revisione

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni o revisioni al presente Regolamento. Le proposte verranno esaminate dalla Direzione Generale congiuntamente al Responsabile dei Sistemi Informativi.
Il presente Regolamento è soggetto a revisione con frequenza annuale.

Dichiarazione di assunzione di responsabilità per l'accesso ad Internet e l'utilizzo della Posta Elettronica dalle postazioni aziendali

(Dichiarazione da sottoscrivere e trasmettere ai Sistemi Informativi)

Il sottoscritto, firmando il presente documento, riconosce di aver letto, compreso ed accettato integralmente le politiche e le regole presenti nel regolamento Aziendale per l'utilizzo delle risorse informatiche, riguardo l'utilizzo e l'accesso ad Internet (punto 7); il sottoscritto si assume la piena responsabilità in caso di violazione delle leggi e dei regolamenti riconducibili al suo accesso personale.

Nome e Cognome: .....

Settore: .....

Firma : .....

Data : .....