# NUOVO MOLINO DI ASSISI SRL

**Gruppo Grigi**

## Policy per l'utilizzo dei *Sistemi Informatici*

## INDICE



Il Presidente

**POLICY PER L'UTILIZZO DEI SISTEMI**
**INFORMATICI AZIENDALI E DEGLI APPARATI DI TELEFONIA**

**Oggetto:** *Informativa e autorizzazione all'utilizzo della strumentazione elettronica; informazioni ed istruzioni relative all'utilizzo degli elaboratori elettronici, delle credenziali di autenticazione, della posta elettronica, della rete Intranet e Internet e dello spazio di memorizzazione di dati e documenti.*

## *Premessa*

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete internet dai dispositivi elettronici, espone **la società** ai *rischi* di un coinvolgimento sia patrimoniale che penale, creando problemi alla sicurezza e all'immagine dell'Azienda stessa.
Premesso che l'utilizzo delle risorse informatiche e telematiche aziendali *deve sempre* ispirarsi ai principi di *diligenza* (com. 1 art. 2104 cc) e *correttezza* (com. 2 art. 2104 cc), atteggiamenti questi destinati a sorreggere ogni atto o comportamento posto in essere nell'ambito del rapporto di lavoro, si ritiene utile adottare regole interne dirette ad evitare comportamenti inconsapevoli e/o scorretti tali da innescare problemi o minacce alla Sicurezza nel Trattamento dei Dati, che legittimano l'esercizio del potere disciplinare (art. 2106 cc e art. 7 Stat. Lav.).

La presente Policy è stata redatta tenendo conto:

- Linee Guida del Garante della Privacy emanate con la delibera n. 13 del 1° marzo 2007 (Gazzetta Ufficiale n. 58 del 10 marzo 2007) e successive m. e/o i.;
- D. Lgs. 30 giugno 2003 n. 196 e del Disciplinare tecnico (Allegato B al citato decreto legislativo) contenente le misure minime di sicurezza;
- Statuto dei Lavoratori L. 20 maggio 1970 n. 300;
- Elaborato: "Smartphone e Tablet scenari attuali e prospettive operative" predisposto dal Garante della Privacy.

Il Presidente

## *1. Entrata in vigore della Policy e pubblicità*

La presente policy entrerà in vigore a partire dalla data di approvazione della stessa da parte dell'Organo di Governo.

L'entrata in vigore della presente Policy comporta il superamento delle precedenti disposizioni adottate in materia, in qualsiasi forma comunicate, che devono intendersi abrogate e sostituite dalla presente.

Copia della presente policy verrà divulgata e resa liberamente consultabile sul server attraverso il sistema intranet e in caso di richiesta o disposizione aziendale potrà essere inoltrata direttamente ai singoli "utenti".

## *2. Campo di applicazione della Policy*

La presente Policy *si applica* a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'azienda a prescindere dal rapporto contrattuale intrattenuto con l'azienda (lavoratori somministrati, collaboratori a progetto, in stage, ecc.).

Ai fini della presente Policy per "***utente***" deve intendersi ogni dipendente e collaboratore (collaboratore a progetto, in stage, agente, ecc.) in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche essere identificata come "*incaricato del trattamento*".

Ai sensi del D. Lgs. n. 196 del 30 giugno 2003 e Reg EUn679/2016, ogni "*incaricato del trattamento*", cui sia stato dato accesso al sistema informativo aziendale mediante credenziali di autenticazione, è *autorizzato* all'utilizzo della strumentazione:

 elettronica (computer, stampanti, fax, scanner, fotocopiatori, dispositivi di rete, etc.),

 telefonica (telefoni a filo, telefoni cordless, telefoni cellulari, smartphone e tablet, ecc.),

 sistema di telefonia,

per lo svolgimento dei compiti assegnati e in particolare per il conseguente trattamento dei dati personali gestiti in ragione delle specifiche mansioni ricoperte e secondo le istruzioni ricevute attraverso la sottoscrizione del contratto di assunzione, la lettera di incarico, Policy aziendale, le informative divulgate etc.

**la società** può effettuare controlli mirati al fine di verificare l'effettivo e corretto adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro, come precisato nei punti 12-13.

Il Presidente

## *3. Utilizzo strumentazione elettronica*

Tutta la strumentazione elettronica e i relativi programmi e/o applicazioni affidati all'utente sono strumenti di lavoro.

Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. La strumentazione elettronica deve essere custodita con cura evitando ogni possibile forma di danneggiamento.

Ogni utente è personalmente e direttamente responsabile dell'uso e della custodia dei dispositivi affidatogli, per cui *deve*:

• custodirli in modo appropriato, non lasciandoli incustoditi;

• proteggerli, sempre, con password e codici identificativi (si rimanda al punto di pertinenza);

• utilizzarli solo per fini professionali e non anche per scopi personali, salvo esplicita deroga,

tanto meno per scopi illeciti;

• segnalare, prontamente, al Servizio CED il loro furto, danneggiamento o smarrimento.

Salvo preventiva ed espressa autorizzazione del personale del Servizio CED, *non è consentito* all'utente:

• modificare le caratteristiche impostate sui dispositivi elettronici,

• installare dispositivi di memorizzazione, comunicazione o altro (come ad es. masterizzatori, modem e dispositivi Bluethooth ecc.);

• accedere contemporaneamente con lo stesso account da più PC;

• collegarsi a siti a pagamento, salvo autorizzazione da funzione legittimata con delega separata;

• effettuare copie di backup su supporti esterni.

Gli strumenti elettronici con connessione ad internet dati in affidamento all'utente sono stati configurati in modo da consentire l'accesso alla rete della **società** solo attraverso specifiche credenziali di autenticazione come chiarito in seguito.

**La società** informa gli "utenti" che il personale incaricato operante presso il servizio *Centro Elaborazione Dati* (CED) (o *Data Center*) di essa **società** è stato autorizzato a compiere interventi sul 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 etc.).

**La società** può effettuare dei controlli mirati (direttamente o attraverso la propria struttura) al fine di verificare l'effettivo e corretto adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro (cfr. artt. 2086, 2087 e 2104 cod. civ.).

Esigenze aziendali potranno anche comportare l'accesso, in un qualunque momento, ai dati trattati da ciascun "utente", ivi compresi gli archivi di posta elettronica. In particolare, il personale incaricato potrà eseguire controlli sui documenti presenti nei pc dei dipendenti, qualora sussista la necessità di:

1. proseguire con l'attività aziendale in assenza del dipendente interessato;

2. rilevare le cause di eventuali anomalie dei sistemi, presenza di virus informatici, esecuzione di manutenzioni, back up;

3. verificare cause di abuso nell'utilizzo degli strumenti elettronici di cui l'azienda si è accorta.



## *3.1 Utilizzo di programmi*

Non è consentito l'uso di programmi diversi da quelli ufficialmente installati, dal personale del Servizio CED, per conto della **società**, 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 di questa disposizione, oltre al rischio di provocare danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'azienda a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (*D. Lgs. 518/92* sulla tutela giuridica del software e Legge a protezione del diritto d'autore e di altri diritti connessi al suo esercizio *Legge 22 aprile 1941, n. 633* e successive modifiche fino al *D. Lgs. 21 febbraio 2014, n. 22*) che impone la presenza nel

sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.

In particolare, *non è consentito*:

- installare programmi non autorizzati dal Servizio CED;
- utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
- modificare le configurazioni impostate sul proprio computer;
- scaricare file contenuti in supporti magnetici, ottici e per drive USB non aventi alcuna attinenza con la propria prestazione lavorativa;
- disinstallare i programmi di protezione: firewalls, antivirus ecc. installati;
- disattivare o bloccare gli aggiornamenti al sistema operativo o antivirus o firewall;
- memorizzare documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

Tutti i file di provenienza incerta ma attinenti all'attività lavorativa, devono essere sottoposti al controllo e relativa autorizzazione di utilizzo da parte del Servizio CED.

## *3.2 Utilizzo Personal Computer (PC*)

Il PC, assegnato ad ogni utente, è uno strumento di lavoro aziendale.

In deroga a tale principio **la società** autorizza un moderato e ragionevole utilizzo privato. Tale utilizzo deve essere limitato ed ispirato a criteri di buon senso e non dovrà ostacolare l'utilizzo professionale.

Lo spazio della risorsa affidata, utilizzato a fini "privati" (ad esempio dislocazione di file dati, foto o filmati), dovrà perciò essere limitato e non dovrà precludere e limitare quello dedicato all'utilizzo Professionale, restando l'assoluto divieto di utilizzo per condotte illecite che possano integrare lesioni del patrimonio aziendale e/o dell'immagine e/o ingenerare delitti informatici e/o illeciti trattamenti dei dati, ivi compreso con specifico rigore, la riproduzione o visione di atti sessuali in genere ed in particolare relativi a minori di età.

Il Personal Computer *deve essere*:

- disattivato e attivato lo screensaver con protezione in caso di allontanamento dalla postazione;
- spento ogni sera prima di lasciare la propria postazione;
- spento in caso di assenze prolungate dall'ufficio;
- spento in caso di non utilizzo prolungato.

Il Presidente

L'utente deve adottare le seguenti misure minime di protezione del dispositivo:

a) utilizzo di programmi vedi punto 3.1;
b) attivazione di credenziali di autentificazioni per l'accesso vedi punto 4;
c) uso di supporti esterni, vedi punto 5;
d) uso della rete aziendale vedi punto 6;
e) uso della posta elettronica aziendali vedi punto 7;
f) navigazione in Internet, vedi punto 8;
g) protezione con software antivirus, firewall ecc., vedi punto 9.

Lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

Il personale incaricato del Servizio CED ha la facoltà di collegarsi e visualizzare in 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, etc.

Tale tipologia di intervento viene effettuato esclusivamente su chiamata dell'utente o, 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, si comunicherà la necessità dell'intervento al dipendente che utilizza normalmente il computer di che trattasi.

Il Presidente

## *3.3 Utilizzo Personal Computer portatili*

L'utente è responsabile del PC portatile assegnatogli dal Servizio CED 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 dal presente regolamento, con particolare attenzione alla rimozione dei file, elaborati prima della riconsegna del dispositivo.

I PC portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

Si invitano gli utenti a non conservare, sui PC portatili o sui supporti esterni, dati aziendali che devono essere backuppati sul server aziendale entro la giornata lavorativa. Tali dati devono poi essere cancellati dal PC o dai supporti.

Il Personal Computer portatile *deve essere*:

- disattivato e attivato lo screensaver con protezione in caso di allontanamento dalla postazione;
- spento in caso di non utilizzo prolungato.

L'utente deve adottare le seguenti misure minime di protezione del dispositivo:

h) utilizzo di programmi vedi punto 3.1;

i) attivazione di credenziali di autentificazioni per l'accesso vedi punto 4;

j) uso di supporti esterni, vedi punto 5;

k) uso della rete aziendale vedi punto 6;

l) uso della posta elettronica aziendali vedi punto 7;

m ) navigazione in Internet, vedi punto 8;

n) protezione con software antivirus, firewall ecc., vedi punto 9.

## *3.4 Utilizzo Tablet e Smartphone*

Tali dispositivi devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

L'utente *deve evitare*:

- di scaricare e installare mobile apps a pagamento o vietate dal Servizio Ced o da market non autorizzati;
- di collegarsi a siti web non attendibili;
- di mettere in carica i dispositivi in docking station non affidabili;
- qualsiasi intervento sul dispositivo con esecuzione del jailbreak che consente lo sblocco del root e la possibilità di modifica del bootloader, al fine di installare versioni alternative del sistema operativo e delle applicazioni;
- di scaricare applicazioni provenienti da app store illecite, non sottoposte a revisioni e verifiche di sicurezza;
- di utilizzare la modalità fotocamera per fini non lavorativi e non diffondere immagini di persone o dati sensibili se non su autorizzazione del Responsabile;
- pubblicare su social network, su siti internet o altro documenti aziendali, foto e video attinenti la propria attività lavorativa e/o pertinente l'azienda, se non su espressa indicazione del responsabile.

L'utente nell'uso quotidiano *deve*:

- bloccare il dispositivo quando non è in uso;
- segnalare al servizio CED i casi di smarrimento o furto del dispositivo per disattivare i certificati e gli altri metodi di accesso a esso associati;
- considerare le implicazioni per la privacy prima di abilitare servizi basati sulla localizzazione e limitare l'uso alle applicazioni non affidabili.

Il Presidente

Si raccomanda inoltre all'utente di predisporre il blocco dei dispositivi mobili attraverso l'inserimento del PIN sulla sim e del codice di blocco del terminale.

Il PIN (Personal Identity Number) è un codice che, se impostato come attivo, viene richiesto dal telefono al momento dell'accensione.

La mancata digitazione del PIN, o l'inserimento per tre volte consecutive del PIN errato, impedisce l'utilizzo della SIM Card non consentendo di telefonare, né di accedere alle funzioni della SIM stessa.

## *3.5 Fenomeno del cd. BYOD (Bring your own Device)*

**La società** si trova spesso a dover gestire richieste provenienti dai dipendenti che chiedono di poter utilizzare i propri dispositivi mobili sul posto di lavoro per lo svolgimento delle loro mansioni assegnate.

Tale fenomeno si riferisce a tutte le tipologie di "lavoratori", comprese le figure professionali rientranti all'interno delle varie forme di rapporto di lavoro parasubordinato (co.co.pro, contratti a progetto, etc.) o autonomo (lavoratori a progetto, consulenti, professionisti ecc.).

Gli utenti non possono scaricare dati sensibili o informazioni riservate dell'azienda all'interno dei propri dispositivi personali, a meno che non siano stati previamente autorizzati dal Servizio CED o scaricate all'interno di una infrastruttura IT di proprietà dell'azienda.

Gli utenti devono notificare al Servizio CED, entro la giornata, ogni effettivo o sospetto avvenimento di hacking e/o di rivelazione non autorizzata di dati contenuti all'interno del dispositivo mobile.

Gli utenti devono garantire un set di requisiti di sicurezza di base da adottare nella configurazione del proprio dispositivo mobile.

Per esempio, la configurazione del dispositivo dovrebbe proibire:

- il back-up o il cloud storage automatico;
- l'utilizzo del dispositivo personale come hotspot mobile;
- l'installazione di alcune specifiche applicazioni particolarmente intrusive e/o illecite (es: jail-break).

L'utente deve effettuare una periodica copia di backup dei propri dati personali in modo tale che in caso di necessità per smarrimento del cellulare il Servizio CED possa provvedere alla cancellazione remota di tutti i dati, per garantire l'integrità delle informazioni sensibili.

Per i dispositivi BYOD l'utente garantisce che non saranno resi accessibili e utilizzati anche dai loro amici e familiari, onde evitare che persone terze possano potenzialmente accedere a tutte le informazioni aziendali archiviate su tali dispositivi.

Mantenere una netta e chiara separazione tra i dati personali trattati per conto dell'Azienda-Titolare del trattamento e quelli trattati per scopi puramente personali del proprietario del dispositivo.

I dati personali trattati attraverso dispositivi mobili non devono risiedere sul dispositivo personale dell'utente ma devono rispettare le procedure di back-up e sincronizzazione dei dati del dispositivo mobile sulla rete aziendale o sul cloud privato aziendale

In caso di smarrimento o sostituzione di dispositivo l'utente deve assicurare e consentire di verificare al Servizio CED che tutti i dati aziendali sensibili siano stati rimossi effettivamente e completamente dal dispositivo.

Attenersi alle indicazioni fornite con l'informativa predisposta dall'azienda.

## *4. Gestione ed assegnazione delle credenziali di autenticazione*

*Indicazioni generali*

Le credenziali di autenticazione per l'avvio dei dispositivi aziendali sono assegnate dal Servizio CED, previa formale richiesta del Responsabile dell'ufficio/area nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente. Nel caso di collaboratori a progetto e coordinati e continuativi la preventiva richiesta, se necessaria, deve essere inoltrata direttamente dal Responsabile dell'ufficio/area con il quale il collaboratore si coordina per l'espletamento del proprio incarico.

Al primo utilizzo sarà cura dell'utente, incaricato del trattamento, procedere alla modifica della parola chiave e, successivamente, ogni **3 mesi**.

La parola chiave (password), formata da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, deve essere composta da almeno otto caratteri.

La password non deve contenere riferimenti agevolmente riconducibili all'incaricato (pertanto non si devono utilizzare nome e cognome o date particolari).

La password dovrà essere custodita in modo tale da:

- evitare accessi ai contenuti del pc da parte di lavoratori non autorizzati al trattamento di dati o informazioni di competenza del titolare della password;
- evitare accessi ai contenuti del pc da parte di soggetti terzi estranei alla struttura.

L'utente dovrà inoltre osservare le seguenti indicazioni:

- non scrivere le password su post-it affissi al pc;
- non comunicare la password via telefono o via mail in caso di mancanza di assoluta certezza circa l'identità della controparte;
- attivare lo Screen Saver protetto da Password;
- predisporre attivazione dello Screen Saver dopo un certo numero di minuti di inutilizzo del computer.

Qualora l'utente venga a conoscenza delle password di altro utente, è tenuto a darne immediata notizia al Servizio CED.

Soggetto preposto alla custodia delle credenziali di autenticazione è il personale incaricato del Servizio CED.

PC fissi

Divieto assoluto di comunicare o diffondere la propria password di accesso al pc.

Comunicazione al Servizio CED della sostituzione di password ogni qualvolta questa sia stato necessario divulgarla per esigenze aziendali al personale**.**

*PC portatili*

Per gli utenti che dispongono di PC portatile o altro dispositivo mobile (es. smartphone, tablet ecc.) il titolare del trattamento dei dati richiede una particolare attenzione nella custodia dello strumento informatico e nello specifico:

- sostituzione e/o immissione della password al primo avvio del dispositivo;
- sostituzione password di avvio del dispositivo ogni 3 mesi ;
- comunicazione al Servizio CED dello smarrimento o perdita del dispositivo.

## 5. *Utilizzo e conservazione dei supporti rimovibili*

Tutti i supporti magnetici rimovibili (dischetti, hard disk esterni, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili nonché informazioni costituenti know-how aziendale, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

In ogni caso, i supporti magnetici contenenti dati sensibili devono essere dagli utenti adeguatamente custoditi, possibilmente in cassetti e armadi provvisti di chiusura. A tal proposito si ricorda che l'utente è responsabile non solo della custodia dei supporti ma anche dei dati aziendali in essi contenuti.

E' vietato l'utilizzo di supporti rimovibili personali.

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale del Servizio CED nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo punto 9 della presente Policy relativa alle procedure di protezione antivirus.

Nel caso di smaltimento, i supporti dovranno essere precedentemente distrutti mediante punzonatura o deformazione meccanica o distruzione fisica o demagnetizzazione.

## 6. *Utilizzo della rete aziendale*

Le unità di rete 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 archiviato, nemmeno per brevi periodi, su queste unità. Si ricorda che per esigenze aziendali, legate a ragioni di salvaguardia e di operatività, sono sottoposte a regolari attività di controllo, amministrazione e backup, da parte del Servizio CED.

Ciascun utente può accedere alla rete aziendale solo attraverso specifica credenziale di autenticazione personale. È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente. In caso si venga a conoscenza di accessi alla rete non autorizzati, l'utente deve immediatamente comunicarla al Servizio CED. Sarà cura del Servizio CED verificare la cosa per bloccare gli accessi non autorizzati ed intraprendere le misure di difesa della rete e del patrimonio aziendale.

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.

Il personale del Servizio CED può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli utenti che sulle unità di rete.

Costituisce buona regola la periodica (almeno ogni tre mesi) 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.

E' severamente vietato collegarsi alla rete aziendale utilizzando mezzi propri come, ad esempio, computer portatili, senza esplicita autorizzazione del Servizio CED.

## 7. *Uso della posta elettronica*

La casella di posta elettronica assegnata all'utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

È fatto divieto di utilizzare le caselle di posta elettronica (es. nome.cognome@nome azienda.it) per motivi diversi da quelli strettamente legati all'attività lavorativa.

Agli utenti addetti al medesimo ufficio/servizio viene assegnata una casella di posta elettronica condivisa.

In questo senso, a titolo puramente esemplificativo, l'utente *non potrà* utilizzare tale posta elettronica per:

- l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es. mp3) se 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, se non per ragioni lavorative;
- la partecipazione a catene telematiche (cosiddette catene di Sant'Antonio). Se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al personale del Servizio CED. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi;
- lo svolgimento di azioni non attinenti alle mansioni assegnate; i responsabili sono tenuti a controllare la posta in arrivo almeno una volta al giorno e devono delegare una persona di fiducia che possa farlo in caso di propria assenza;

- tutte le caselle di posta elettronica sono oggetto di salvataggio automatico sia per le comunicazioni in ingresso che in uscita.
- inviare, anche all'interno della rete aziendale, materiale a contenuto violento, sessuale o comunque offensivo dei principi di dignità personale, di libertà religiosa, di libertà sessuale o di manifestazione del pensiero, anche politico. Inviare messaggi di POSTA ELETTRONICA, anche all'interno della rete aziendale, che abbiano contenuti contrari a norme di legge ed a norme di tutela dell'ordine pubblico, rilevanti ai fini della realizzazione di una fattispecie di reato, o che siano in qualche modo discriminatori della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap. Qualora il dipendente riceva messaggi aventi tali contenuti, è tenuto a cancellarli immediatamente e a darne comunicazione tempestiva al Servizio Ced.

La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili, non pertinenti all'attività lavorativa e soprattutto allegati ingombranti.

La documentazione elettronica che costituisce per l'azienda "know how" aziendale tecnico o commerciale protetto e che, quindi, viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto a tutela del patrimonio dell'impresa, non può essere comunicata all'esterno senza preventiva autorizzazione della Direzione.

**La società** consente per ragioni di operabilità di visualizzare le e-mail aziendali anche su supporti personali. L'utente deve però attenersi alle medesime indicazioni comportamentali e alle misure di tutela previste nel caso dell'utilizzazione di strumentazione aziendale.

Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per **la società** ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere visionata od autorizzata dal Responsabile d'ufficio e salvata sul server aziendale.

Il Presidente

Si evidenzia che le comunicazioni ufficiali, da inviarsi mediante gli strumenti tradizionali (fax, posta, PEC …), devono essere autorizzati e/o firmati dalla Direzione e/o dai Responsabili di ufficio, a seconda del loro contenuto e dei destinatari delle stesse.

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).

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.

Sarà comunque consentito al superiore gerarchico dell'utente visionare tramite persona delegata (fiduciario) la casella di posta elettronica per verificare il contenuto dei messaggi ed inoltre al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Di *tale attività viene redatto verbale* che sarà sottoposto al lavoratore interessato alla prima occasione utile.

Il contenuto degli account di posta elettronica disattivati sarà registrato in un file di backup. Successivamente alla cessazione del rapporto di lavoro, la Società potrà liberamente accedere al contenuto del file di backup, del personal computer nonché alla casella di posta elettronica assegnata al lavoratore durante il rapporto di lavoro per ragioni di continuità dell'attività della Società, per finalità di sicurezza del sistema informatico, nonché quando ciò sia necessario nei casi indicati ai punti 12 e 13.

## 8. *Navigazione in Internet*

Il dispositivo abilitato alla navigazione in Internet costituisce strumento aziendale necessario allo svolgimento dell'attività lavorativa assegnata. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.

All'utente *non* è consentito:

- accedere a siti INTERNET evitando o superando o comunque tentando di superare o disabilitando i sistemi adottati dalla società per bloccare l'accesso ad alcuni siti ed in ogni caso utilizzare siti o altri strumenti (es. CRACKING PROGRAMS) che realizzino tale fine.
- 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.



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 per prevenire determinate operazioni quali l'upload o l'accesso a determinati siti considerati non pertinenti all'attività operativa, pertanto inseriti in una black list.

Il servizio di connessione internet aziendale non deve essere utilizzato per commettere azioni punibili o reprensibili quali ad esempio infrangere i diritti di proprietà intellettuale e visitare siti pornografici.

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, anche filmati e musica, provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà venir a tal fine contattato il personale del Servizio CED);
- 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 dalla Direzione Generale (o eventualmente dal Responsabile d'ufficio e/o dal Servizio CED) 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 nicknames) se non espressamente autorizzati dal Responsabile d'ufficio;
- l'accesso, tramite internet, a caselle webmail di posta elettronica personale.

Gli eventuali controlli, compiuti dal personale incaricato del Servizio CED, potranno avvenire mediante un sistema di controllo dei contenuti (*Proxy server*) o mediante "*file di log*" della navigazione svolta.

Il controllo sui file di log non è continuativo ed i file stessi vengono conservati non oltre il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'azienda.

I files privati scaricati sul pc dall'utente non saranno oggetto di cancellazione da parte del Servizio CED, qualora possano essere eventualmente presentati come prova in un eventuale contenzioso giudiziario.

## *9. Protezione antivirus*

Il sistema informatico è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o altro software aggressivo.

Ogni utente è tenuto a controllare il regolare funzionamento e aggiornamento periodico del software installato secondo le procedure.

Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente:

a) sospendere ogni elaborazione in corso senza spegnere il computer,

b) segnalare prontamente l'accaduto al personale del Servizio CED.

Ogni dispositivo magnetico di provenienza esterna all'Azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale del Servizio CED.

## *10. Utilizzo dei telefoni, fax e fotocopiatrici aziendali*

*Indicazioni generali*

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 l'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali è consentito solo nel caso di comprovata necessità ed urgenza. In generale, i telefoni non possono essere ceduti né fatti utilizzare a terzi, eccetto colleghi, collaboratori, consulenti o soggetti identificati ed autorizzati.

I dati di traffico, acquisiti dal sistema di telefonia, sono utili per la validazione dei prospetti di consumo, che le compagnie telefoniche addebitano, sulla base dei tabulati telefonici da esse riscontrati. Pertanto, l'operazione di trattamento dei dati di traffico mira principalmente a verificare la sussistenza e la veridicità dei conti telefonici. Potrebbe emergere dall'analisi primaria un interesse ad approfondire la genesi dei costi ed eventualmente a verificare il corretto utilizzo dei telefoni aziendali.

Pertanto, *è facoltà del Titolare effettuare controlli mirati all'individuazione di condotte illecite o vietate, ricorrendo sia ai tabulati telefonici, sia ai dati di traffico registrati dal sistema di telefonia interno, mediante operazioni di analisi, selezione e raffronto*.

In caso di guasti o malfunzionamenti, l'utilizzatore dovrà rivolgersi al Servizio CED a cui è demandata la relativa gestione in queste circostanze.

*Cellulare aziendale*

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 (indicazioni generali) 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 di natura personale o comunque non pertinenti rispetto allo 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 del Servizio CED.

Quanto memorizzato sui supporti interni al telefono potrebbe essere oggetto di analisi, controllo e duplicazione da parte del Servizio CED, per migliorare l'affidabilità, la disponibilità e l'efficienza del dispositivo.

Qualora fossero individuate componenti hardware e/o software (programmi, documenti, dispositivi esterni, ecc.) non corrispondenti ai criteri di sicurezza e di operatività non esplicitamente autorizzati, tali componenti potrebbero essere rimossi e l'utilizzatore potrebbe essere coinvolto negli accertamenti e nelle verifiche del caso.

In particolare, in modo non esaustivo, si intende stigmatizzare i comportamenti relativi ai seguenti divieti:

- non è consentito modificare le caratteristiche hardware e software impostate sul telefono,
- non è consentita l'installazione di programmi diversi da quelli autorizzati,
- non è consentita la riproduzione, la duplicazione, il salvataggio o lo scarico (download o file sharing) di programmi o file di ogni tipo (testo, immagini, video, audio, eseguibili) in violazione delle norme sul diritto d'autore, ai sensi delle Legge n. 128 del 21 maggio 2004,
- non è consentita l'installazione di ulteriori dispositivi rispetto a quelli in dotazione,

- non è consentito utilizzare la fotocamera o videocamera del dispositivo per effettuare foto o video non pertinenti l'attività operativa e la loro divulgazione su social network o in internet, per qualsiasi finalità.

L'utilizzatore che abbia necessità di apportare modifiche software o hardware al telefono in dotazione, installando nuovi programmi o dispositivi, deve farne preventiva richiesta al Servizio CED.

In caso di furto o smarrimento o danneggiamento dei telefoni, l'utilizzatore deve dare tempestiva comunicazione al Servizio CED, rimanendo a disposizione nel caso sia necessario denunciare l'accaduto all'Autorità preposta.

*Fax, fotocopiatrici, stampanti*

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.

Per quanto concerne l'utilizzo delle stampanti, gli utenti sono tenuti a stampare documenti e atti solo se strettamente necessari per lo svolgimento delle proprie funzioni lavorative.

Qualora il dipendente dovesse stampare documenti contenenti dati o informazioni riservate, dovrà aver cura di monitorare la stampante e preservare, limitatamente alle oggettive possibilità, la conoscibilità di tali dati o informazioni da parte di terzi non autorizzati.

È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. È buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio il formato pdf o file di contenuto grafico) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.



## *11. Osservanza delle disposizioni in materia di Privacy*

È obbligatorio attenersi alle disposizioni in materia di Privacy e in particolare, fatte salve successive modificazioni e/o integrazioni, alle misure:

- minime di sicurezza, come indicato nella lettera di designazione ad incaricato del trattamento dei dati ai sensi del Disciplinare tecnico allegato al D. Lgs. n. 196/2003 e REG EU 679/2016;
- sicurezza e salute sul lavoro in particolare a quanto dispone l'art. 20 del D. Lgs. 81/2008 e smi;
- copyright in particolare Legge 22.04.1941 n° 633, G.U. 16.07.1941 con successive modifiche in particolare: D. Lgs. 21 febbraio 2014, n. 22;
- delitti in materia di violazione del diritto d'autore: Art. 25-novies D. lgs. 231/2001;
- delitti informatici e trattamento illecito di dati: Art. 24-bis D. lgs. 231/2001.

## *12. Accesso ai dati trattati dall'utente*

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 della Direzione Aziendale, tramite il personale del Servizio CED 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.

Si possono determinare, inoltre, forme di intervento, controllo o monitoraggio diretti ad accertare condotte illecite che potrebbero integrare lesioni del patrimonio aziendale o della sicurezza o illeciti contrattuale o di forma di illeciti.

In ogni caso l'accesso a strumenti informatici in affidamento a terzi (dipendenti, collaboratori, ecc.) dovrà essere preceduto dall'invito al soggetto affidatario affinché possa assistere alle operazioni da effettuarsi.

## *13. Sistemi di controlli graduali*

L'azienda si riserva la facoltà di attuare controlli per verificare l'integrità del sistema informatico, per la sua ordinaria manutenzione, per accertare e segnalare eventuali abusi dei lavoratori che possono essere fonte di danneggiamento per il patrimonio, l'immagine, la strumentazione, la privacy trattata dall'azienda.

Nel caso in cui si verificassero dei problemi di natura tecnica quali guasti o malfunzionamenti, l'azienda incaricherà dei tecnici specializzati al fine di rilevare risolvere le cause dei guasti o i malfunzionamenti, con la possibilità di ravvedere ragioni per un'analisi approfondita dell'utilizzo del dispositivo.

Nel caso di malfunzionamento dei dispositivi, degli account di posta e rete internet, si potrà accedere ai dati riferibili a cookies, indirizzi IP, nome domini visitati, analisi della posta elettronica, allegati, download, account e qualunque file utile alla soluzione del problema.

In ogni caso l'azienda utilizzerà impianti hardware e software quali firewall, antispam, antivirus e altri strumenti di controllo passivo, con sistemi di filtraggio che consentono il blocco totale o parziale di determinati accessi a siti internet e che garantiscano la sicurezza di eventuali intrusioni illecite dall'esterno.

Le strutture di controllo potrebbero raccogliere dati come indirizzi IP, cronologie, ping, cookie e altri dati di cui si effettuerà il trattamento in forma anonima.

I controlli sono effettuati al fine di verificare la sicurezza del sistema e per garantire la corretta manutenzione e saranno attuati nel pieno rispetto della privacy dei lavoratori e delle regole sul corretto trattamento dei dati personali che dovessero essere gestiti dall'Azienda.

I controlli predisposti dal Servizio CED avranno la finalità di accertare:

1. utilizzo per scopi privati o impropri del dispositivo e degli accessi ad Internet concessi all'utente per verificare abusi di utilizzo nella connessione;
2. la non conformità dell'utente agli obblighi contrattuali in tema di uso corretto degli strumenti affidati sul luogo di lavoro e di conseguenza della destinazione d'uso delle risorse aziendali.

Qualora dal controllo preliminare si accertasse un abuso, l'azienda si riserva di effettuare un controllo di approfondimento con specifica indagine dei contenuti dei file o delle connessioni o delle mail aziendali secondo le seguenti procedure:

a) presenza dell'interessato e/o persona da lui delegata;

b) presenza di personale all'uopo designato ed incaricato, previa informativa all'utente interessato affinché possa proporre le proprie ragioni.

I dati desunti e rilevati, durante i controlli, saranno conservati per il tempo utile e strettamente limitato al perseguimento di finalità organizzative e sicurezza per adozione di misure disciplinari ed eventualmente contestazione giudiziaria.

## *14. Cessazione o sospensione del rapporto di lavoro*

Nel caso in cui cessi il rapporto di lavoro o di collaborazione, l'utente incaricato del trattamento deve:

- consegnare i beni aziendali in dotazione (telefono e computer portatili, chiavette USB, etc.),
- assicurarsi che i files e i documenti elettronici di rilevanza aziendale siano presenti sul server.

Il Presidente

E' compito del Sistema CED, in seguito alla cessazione di un rapporto di lavoro:

- effettuare il ripristino alla configurazione iniziale (reset) dei beni aziendali dotati di sistema operativo;
- disattivare le credenziali di autenticazione sui server;
- cancellare definitivamente i dati con sistemi di remote kiping una volta che il dispositivo debba essere rottamato.

## *15. Sanzioni*

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 dell'art. 13 del D. Lgs. 30 giugno 2003 n. 196, in conformità a quanto disposto dalla Provvedimento n. 13 del 1° marzo 2007 dell'Autorità Garante per la privacy, si ritiene necessario informare che:

- il titolare, attraverso il proprio Servizio CED, può effettuare un monitoraggio periodico dell'hardware e del software installato negli elaboratori aziendali. Tale operazione viene effettuata, in modo completamente automatico per le macchine in rete ed in modo semiautomatico per le macchine stand-alone, mediante l'utilizzo di apposito software installato o da installare in ogni computer aziendale. 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 computer, ma permette la rilevazione dì software installato in violazione di questa policy;
- 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 files multimediali non attinenti all'attività lavorativa;
- eventuali comportamenti anomali saranno segnalati genericamente alle aree interessate (uffici, servizi) e, solo qualora tali comportamenti dovessero continuare, la Direzione potrà procedere, nel rispetto delle norme legali e contrattuali, a controlli individuali.

Il trattamento dei dati, così come descritto, è obbligatorio, pena l'impossibilità di utilizzare qualunque elaboratore informatico.

I dati personali saranno trattati nel rispetto delle modalità indicate nell'art. 11, il quale prevede, tra l'altro, che i dati stessi siano trattati in modo lecito e secondo correttezza, raccolti e registrati per scopi determinati, espliciti e legittimi, esatti, e se necessario aggiornati, pertinenti, completi e non eccedenti rispetto alle finalità del trattamento, nel rispetto delle norme minime di sicurezza previste dall'Allegato B.

È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente CCNL nonché con tutte le azioni civili e penali consentite.

Gli utenti possono esercitare i diritti di cui all'art. 7, tra cui conferma dell'esistenza, rettifica, integrazione e cancellazione dei dati.

## *16. Aggiornamento e revisione*

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate alla presente Policy. Le proposte verranno esaminate dalla Direzione Generale.

La presente Policy è soggetta a revisione con tempistiche determinate dalle esigenze aziendali ed organizzative o quando si presenti la necessità di un suo adeguamento alle mutate condizioni aziendali.

*addì* …….

*Il Presidente*

Il Presidente