POLICY SULL' UTILIZZO DELLE ATTREZZATURE INFORMATICHE, DELLE MAIL, DELLA NAVIGAZIONE INTERNET, DELLA RETE AZIENDALE

FINALITA' E AMBITO DI APPLICAZIONE

Fornire procedure e misure idonee di sicurezza per il corretto utilizzo da parte di ciascun dipendente degli strumenti informatici, della posta elettronica aziendale e della navigazione sulla rete Internet.

DESTINATARI

Al fine di garantire la tutela dei diritti e delle libertà degli interessati, la presente Policy è messa a disposizione e deve essere osservata dai seguenti soggetti:

- Responsabile della protezione dei Dati (DPO)
- Dirigenti designati e lavoratori Incaricati dal Titolare per le sole finalità e con le modalità connesse alle loro responsabilità e mansioni lavorative
- Responsabili esterni del titolare per le sole finalità e con le modalità connesse alle loro responsabilità e obbligazioni contrattuali

INOSSERVANZA

L' inosservanza delle norme contenute in questa Policy costituisce inadempimento contrattuale al quale potranno far seguito le misure previste dal titolare del trattamento quali, per i dipendenti: sanzioni disciplinari sino al licenziamento, per i terzi risoluzione del contratto di servizio, richieste risarcitorie in ordine ai danni causati. Rimane salva l'eventuale responsabilità penale per gli autori dell'illecito.

UTILIZZO DEL PERSONAL COMPUTER

Il personal computer (portatile o fisso) affidato a ciascun Dipendente, Collaboratore o Terzo è da intendersi esclusivamente "strumento di lavoro", in forza di ciò è vietato ogni suo utilizzo che non sia strettamente necessario ed inerente all' attività lavorativa. Ognuno è responsabile della custodia e del corretto utilizzo delle apparecchiature informatiche concesse in uso dal titolare. Alla luce di ciò, salvo specifiche autorizzazioni della Direzione del personale e con l'intervento del Responsabile IT, è fatto esplicito divieto di:

- Modificare qualsiasi caratteristica hardware e software preimpostata dai sistemi IT sul proprio personal computer;
- installare e/o eseguire qualsiasi tipologia di programmi informatici diversi da quelli preinstallati dal titolare, anche nel caso si tratti di software opportunamente licenziato, di software in prova ("shareware"), ovvero di software gratuito o liberamente scaricabile da Internet ("freeware");
- scaricare da internet, copiare e/o archiviare- anche temporaneamente- sul personal computer in dotazione qualsiasi file audio, video, eseguibile, ecc. (l'elencazione è esemplificativa e non esaustiva) non necessario allo svolgimento dell'attività lavorativa;
- effettuare visualizzazioni di file di qualunque tipo di in streaming, salvo ciò che non sia necessario per fini lavorativi e previa informativa al Responsabile IT;
- effettuare sul pc in dotazione il backup ovvero la sincronizzazione di apparecchi smartphones, tablet;
- utilizzare dispositivi di archiviazione di massa quali hard disk esterni e/o Pen drive;

- cedere a soggetti non autorizzati il proprio personal computer, soprattutto successivamente al superamento della fase di autenticazione;
- lasciare incustodito e accessibile il proprio personal computer senza aver precedentemente provveduto a bloccare l ' accesso alla postazione attraverso l ' apposito comando (CTRL+ALT+CANC e successivamente cliccare su "Blocca il computer"), al fine di evitarne un utilizzo improprio in caso di assenza anche temporanea. In ogni caso, dopo un periodo congruo di inutilizzo della postazione di lavoro, l'accesso verrà bloccato in automatico;
- archiviare i files inerenti le attività lavorative sui dischi locali del personal computer assegnato; tali files dovranno essere conservati e salvati esclusivamente nelle apposite aree di rete;
- eliminare o comunque rendere inaccessibile qualsiasi tipologia di informazione lavorativa dal proprio personal computer in caso di cessazione del rapporto di lavoro.

E' fatto obbligo ad ogni utilizzatore di provvedere allo spegnimento delle postazioni di lavoro, al termine della giornata lavorativa, salvo espliciti e contrari avvisi da parte degli addetti ai sistemi informatici.
Ogni utente è avvisato ed ha contezza del fatto che le informazioni presenti all' interno del personal computer (PC) assegnato, trattandosi di "strumento di lavoro", siano considerate e trattate come lavorative e non personali. Pertanto, in conformità coi principi di necessità, pertinenza e non eccedenza della normativa sul trattamento dei dati personali, il titolare si riserva fin da ora il diritto di poter eventualmente accedere in qualunque momento alle informazioni e ai dati presenti al suo interno per esclusive finalità lavorative, di continuità operativa dell'azienda e/o di salvaguardia dei propri diritti in sede Giudiziaria.
Ogni utente è responsabile del personal computer portatile eventualmente assegnatogli, tale bene aziendale dovrà essere custodito con diligenza ed attenzione soprattutto in occasione di utilizzo al' esterno delle strutture aziendali, in tali occasioni il computer portatile non dovrà mai essere lasciato incustodito ovvero dovrà esser riposto in luoghi ove siano attive le misure più idonee per la sua protezione.
In caso di furto o smarrimento, l'utente assegnatario del personal computer ha l'obbligo d' informare immediatamente e senza ritardo il proprio diretto responsabile di funzione e gli addetti ai sistemi IT, nonché di denunciare tempestivamente l'accaduto alle Forze dell'Ordine, fornendo al titolare, entro x ore dall' evento copia dell'atto di denuncia che dovrà indicare marca e modello dello strumento.
Il titolare si riserva di provvedere-in qualsiasi momento ed anche senza alcun preavviso- alla rimozione di ogni file o software o applicazione che si ritenessero dannosi o pericolosi per la sicurezza ovvero che violino le regole previste all' interno della presente Policy o che, in ogni caso, possano costituire alterazione della configurazione originaria dello strumento di lavoro.

ASSENZE DEL LAVORATORE

Solo l'utente abilitato può accedere alla propria postazione informatica utilizzando le proprie credenziali di autenticazione.

L' eccezione a questa regola ricorre solo nel caso in cui si verifichino contemporaneamente le seguenti tre condizioni:

- una prolungata assenza o prolungato impedimento del lavoratore;
- l'accesso ai dati e agli strumenti elettronici del lavoratore assente risulti essere indispensabile e indifferibile;
- l'accesso ai dati e agli strumenti elettronici del lavoratore assente sia caratterizzato da concrete necessità di operatività e di sicurezza del sistema.

Solo al verificarsi delle tre condizioni sopra esposte, il Titolare del trattamento potrà chiedere il reset della password all' Amministratore di sistema. Della procedura sopra descritta e di ogni attività eseguita verrà redatto a cura del Titolare del trattamento un apposito verbale e il lavoratore interessato verrà prontamente informato dell'accaduto alla prima occasione utile.

GESTIONE DELLE PASSWORD.

L ' accesso a ogni postazione di lavoro informatica è governato da un sistema d' identificazione personale basato sull' utilizzo di credenziali di accesso (consistenti in una e più accoppiate di username e password), che ne permettono l'utilizzo nei modi e nelle forme definite da ciascun profilo aziendale esclusivamente agli utenti autorizzati.
Le credenziali di accesso sono e devono essere conosciute esclusivamente dal soggetto o dai soggetti per i quali sono state predisposte

La parola chiave (password) deve essere composta da almeno x (xx) caratteri alfa numerici (lettere minuscole, maiuscole e numeri), meglio se con l ' aggiunta di caratteri "speciali". Non dovrà contenere, inoltre, riferimenti direttamente riconducibili al lavoratore e deve essere obbligatoriamente rimpiazzata al suo primo utilizzo e, successivamente, almeno ogni x (x) mesi.
L' utente è tenuto a conservare nella massima segretezza la parola di accesso e/o qualsiasi altra informazione legata al processo di autentificazione/autorizzazione e a modificare immediatamente la password nel caso in cui sia a conoscenza che la stessa abbia perso il suo carattere di segretezza e che possano in conseguenza di ciò essere state commesse violazioni informatiche il medesimo dovrà dame immediata comunicazione all' Amministratore di Sistema e al Responsabile dei Sistemi IT.
Le credenziali di autenticazione saranno comunque prontamente disattivate in caso di perdita della qualità che consente al soggetto l'accesso ai dati aziendali e/o personali.
Di ogni azione o attività svolta utilizzando il codice identificativo e/o la password assegnata è responsabile l' utente o il gruppo di utenti assegnatari de codice, che ne rispondono nei confronti del titolare ed eventualmente nei confronti di terzi.

USO DELLA RETE TELEMATICA AZIENDALE.

La rete telematica aziendale è l 'insieme delle tecnologie – hardware e software- mediante le quali si realizza la connettività interna tra i vari componenti del sistema informatico aziendale. La perfetta e continuativa disponibilità della stessa è quindi fattore strategico per il funzionamento operativo di ogni Azienda.
Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi da quelli per cui sono state predisposte. Pertanto, qualunque file che non sia legato all' attività lavorativa non può essere dislocato- nemmeno temporaneamente- in dette unità di rete.
E' fatto assoluto divieto di entrare nella rete interna e nei programmi utilizzando credenziali di autenticazione di qualsiasi altro utente, tranne per casi di utenze di lavoro condivise.
L' Amministratore di Sistema, anche senza preavviso, può in qualunque momento procedere alla rimozione di ogni file o applicazione che dovesse ritenere pericolosa per la sicurezza, sia sui PC dei lavoratori che sulle unità di rete.
Alla luce di quanto evidenziato, è fatto esplicito divieto di:

- ✓ utilizzare la rete interna aziendale per fini non espressamente previsti e/o autorizzati e per scopi che non siano strettamente lavorativi;
- ✓ connettere in rete locale apparecchiature elettroniche (PC, stampanti, ecc.) o qualsiasi altro genere di apparato (router, switch; ecc) che possa alterare la configurazione della rete interna e/o danneggiare le applicazioni.

Il titolare si riserva fin da ora il diritto di rimuovere, in qualunque momento e anche senza alcun preavviso, qualsiasi tipologia di apparecchiatura elettronica o di software installato sulla rete interna aziendale e che non sia stato in precedenza autorizzato.

USO DELLA POSTA ELETTRONICA TRADIZIONALE E CERTIFICATA

La casella di posta elettronica tradizionale e/o di posta elettronica certificata (PEC) assegnata dal titolare a ciascun soggetto o a gruppi di utenti è uno "strumento di lavoro". Gli assegnatari di una o più caselle di posta elettronica (tradizionale o certificata), pertanto, sono responsabili del loro corretto utilizzo
Essendo esclusivamente uno strumento di lavoro, ogni utente è avvisato che le informazioni presenti all' interno della casella di posta elettronica aziendale assegnata (tradizionale/o certificata) sono considerate e trattate come corrispondenza e documentazione lavorativa e non personale. Pertanto, in conformità con i principi di necessità, pertinenza e non eccedenza, il titolare si riserva fin da ora il diritto di poter eventualmente accedere in qualunque momento alle informazioni ai dati presenti al loro interno per esclusive finalità lavorative, di continuità operativa dell'azienda e/o di salvaguardia dei propri diritti in sede Giudiziaria.
Si precisa, inoltre che la casella di posta elettronica certificata (PEC) ha valore legale. Pertanto, ogni utilizzo improprio da parte di qualsivoglia utente verrà valutato alla luce delle specifiche normative vigenti.
Il titolare, pur proteggendo con le più adeguate misure di sicurezza i sistemi di gestione delle caselle e-mail da messaggi potenzialmente pericolosi, fa comunque divieto a tutti gli utenti di:

- ➢ utilizzare l'indirizzo di posta elettronica aziendale per l ' iscrizione e la partecipazione a dibattiti, forum o mailing- list, ecc.., salvo comprovate esigenze lavorative;

- utilizzare l'indirizzo di post elettronica aziendale per l 'invio di messaggi completamente estranei al rapporto di lavoro o alle normali interrelazioni lavorative tra colleghi;
- utilizzare l ' indirizzo di posta elettronica aziendale per attività improprie;
- aprire email e/o gli allegati che abbiano solo un contenuto insolito; in caso di dubbio è fatto obbligo di avvisare preventivamente gli addetti ai sistemi informatici che daranno istruzioni in merito;
- inviare o dare corso a catene telematiche di messaggi cosiddette ("Catene di Sant' Antonio").

Il titolare fa obbligo a tutti gli utenti dotati di account e-mail di:

- utilizzare le apposite funzionalità di sistema che, in caso di assenza, consentono di inviare automaticamente messaggi di risposta contenenti il recapito (elettronico e/o telefonico) di un altro lavoratore ovvero delle altre modalità utili a contattare il titolare;
- in caso di eventuali assenze non programmate, qualora il soggetto non possa inviare la procedura sopra descritta, il titolare si riserva di disporre lecitamente l'attivazione un analogo accorgimento attraverso i Sistemi IT, dandone comunicazione all' interessato
- mantenere in ordine la casella di posta elettronica, provvedendo alla cancellazione dei documenti superflui e, soprattutto, degli allegati non più utili ai fini lavorativi.

Il titolare, infine, si riserva in qualunque momento il diritto di procedere alla rimozione di ogni file si dovesse ritenere pericoloso per la sicurezza del patrimonio informativo aziendale o che, ad ogni modo, alteri la configurazione originaria della posta elettronica dell'utente.

USO DELLA RETE INTERNET

La rete Internet e la navigazione sul web sono diventati uno strumento di comunicazione e di informazione anche in ambito lavorativo, il personal computer abilitato alla navigazione web costituisce a tutti gli effetti uno "strumento di lavoro" necessario allo svolgimento dell'attività lavorativa.
Il Titolare ha provveduto a:

- individuare le categorie di siti considerate non correlate con la prestazione lavorativa;
- impedire la navigazione su detti siti attraverso un sistema di filtri sulla navigazione e sulle attività ritenute potenzialmente dannose;
- predisporre nel tempo la conservazione dei dati strettamente limitati al perseguimento di finalità organizzative, produttive e di sicurezza.

L' utente è direttamente responsabile dell'uso del servizio di accesso ad Internet, dei contenuti che vi ricerca, dei siti che contatta, delle informazioni che vi immette e ì, più in generale, delle modalità con cui opera. Il prelievo (download)o la consultazione online anche in streaming di immagini, file musicali, file video o di qualsiasi altra informazione non attinente all' attività non è consentito. Il prelievo (download) o la consultazione online anche in streaming di immagini, file musicali, file video e in ogni caso di grandi quantità di dati per scopi lavorativi che possono compromettere le performance della rete, debbono essere precedentemente concordate con gli addetti dei sistemi informativi.

All' utente pertanto, non è concesso di:

- servirsi o dar modo ad altri di servirsi della postazione di accesso ad Internet per attività poste in essere in violazione del diritto d' autore o altri diritti tutelati dalle norme vigenti;
- utilizzare sistemi di file sharing, podcasting, web casting, se non per scopi connessi con l'attività lavorativa;
- utilizzare qualsiasi genere di social media, social network e/o forum, ad eccezione di quelli appositamente predisposti e autorizzati dal Titolare del trattamento;
- utilizzare Internet Provider diversi da quello predefinito dal Titolare e connettere la propria postazione di lavoro aziendale alle reti di tali Provider con sistemi di connessione diversi da quello centralizzato (ad es., attraverso modem. Internet key, ecc)

PROTEZIONE ANTIVIRUS

Ogni soggetto deve collaborare fattivamente con il titolare per ridurre al minimo il rischio di attacchi ai sistemi informatici aziendali attraverso software malevoli (ad es., worm, virus, trojan, ecc.) e, più in generale, attraverso l 'azione di programmi di cui all' art. 615 – quinquies del Codice Penale, aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi

in esso contenuti o ad esso pertinenti, ovvero l ' interruzione totale o parziale, o alterazione del suo funzionamento.

Ogni utente, pertanto è tenuto a:

- ❖ tenere costantemente attiva la protezione antivirus;
- ❖ segnalare ai servizi IT l ' irregolare funzionamento del software antivirus installato;
- ❖ contattare prontamente i Servizi IT nel caso in cui il software antivirus non riesca automaticamente ad eliminare la minaccia dai sistemi aziendali
- ❖ verificare con il software antivirus, prima dell'apertura di qualsiasi file, ogni dispositivo (ad es., chiavette USB, DVD, CD, hard disk esterni, ecc.) provenienti dall' esterno della struttura.

Il titolare si riserva fin da ora il diritto di implementare su ogni postazione elettronica programmi che impediscano l'installazione e la diffusione di software potenzialmente dannoso per la sicurezza della rete aziendale. La rimozione e/o la disattivazione non autorizzata di detti programmi è assolutamente vietata.

UTILIZZO DI APPARATI DI TELEFONIA MOBILE PER NAVIGAZIONE ATTRAVERSO RETE MOBILE

L' utilizzo di ogni apparato e della SIM aziendale dovrà sempre essere realizzato nel rispetto dei principi di diligenza, correttezza e buona fede, con l 'osservanza delle norme di legge.

Ogni lavoratore- Socio, Dipendente, Collaboratore o Terzo- ha il diritto di utilizzare il dispositivo mobile assegnato anche per uso personale nei limiti della modalità prescelta.

Al momento della restituzione o in caso di cessazione del rapporto di lavoro per qualsivoglia ragione, l' utilizzatore ha l' obbligo di cancellare qualsiasi informazione di natura personale registrata all'interno del dispositivo, ivi compresi, a titolo esemplificativo e non esaustivo, nomi e cognomi, numeri di telefono, messaggi, fotografie, video e quant' altro sia conservato al suo interno. In mancanza saranno gli addetti dei Sistemi IT ad effettuare – senza preavviso e alla prima occasione utile- questa operazione, operando attraverso procedimenti di hard reset e senza mai accedere ai contenuti all' interno dei dispositivi.

In caso di furto o smarrimento, l'utente assegnatario dello smartphone o del tablet ha l'obbligo d' informare immediatamente e senza ritardo il proprio diretto responsabile di funzione e gli addetti ai sistemi IT, nonché di denunciare tempestivamente l'accaduto alle Forze dell'Ordine, fornendo entro 24 ore dall' evento copia dell'atto di denuncia che dovrà indicare marca, modello e codice IMEI del dispositivo.

E' fatto obbligo che ciascun dispositivo venga protetto dal suo utilizzatore quantomeno attraverso un codice PIN ovvero parola chiave (password) che, nei limiti di quanto tecnicamente possibile, dovrà seguire le regole dettate in precedenza all' interno del paragrafo XXX ("Gestione delle password").

MONITORAGGIO E CONTROLLI

Nel caso si renda necessario effettuare dei controlli sull' uso degli strumenti elettronici, saranno rispettati i principi di pertinenza e non eccedenza degli stessi, onde evitare un'interferenza ingiustificata sui diritti e le libertà fondamentali dei soggetti interni nonché dei soggetti esterni che ricevono inviano comunicazioni elettroniche.

Nel caso in cui un evento dannoso o una situazione di pericolo non sia stato impedito con preventivi accorgimenti tecnici, il titolare metterà in atto le opportune misure tecniche e tecnologiche volte alla verifica dei comportamenti anomali secondo la seguente procedura:

- sarà preferito, per quanto possibile, un controllo preliminare sui dati aggregati e anonimi, riferiti all' intera struttura lavorativa o a sue specifiche aree;
- il controllo anonimo si concluderà con un avviso generalizzato relativo al rilevato utilizzo anomalo degli strumenti elettronici aziendali e con l ' invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite attraverso la presente Policy e le ulteriori normative aziendali interne. L' avviso potrà anche essere circoscritto a Dipendenti, Collaboratori o Terzi afferenti all' area o settore in cui è stata rilevata l ' anomalia;
- in caso di perdurare delle anomalie, sarà ritenuto giustificato porre in essere gli opportuni controlli su base individuale, che, ad ogni modo non potranno essere prolungati oltre il tempo ragionevole per lo svolgimento dell'accertamento, ovvero essere costanti e indiscriminati.