REGOLAMENTO AZIENDALE

PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI

DI ASF SAN GIULIANO MILANESE

Premessa

***

Gli strumenti informatici rappresentano da un lato un mezzo insostituibile di lavoro (se adoperati nel rispetto del principio della diligenza e correttezza) e dall'altro lato un rischio per la sicurezza del patrimonio aziendale (se utilizzati in modo non idoneo).

Si rende pertanto necessaria l'adozione da parte di ASF SAN GIULIANO MILANESE del presente Regolamento aziendale finalizzato a disciplinare il regolare utilizzo dei predetti strumenti, con particolare riferimento alle seguenti problematiche:

1) utilizzo del computer (fisso e portatile)
2) gestione della password
3) utilizzo della rete (aziendale e internet)
4) utilizzo della posta elettronica
5) protezione
6) salvataggio
7) smaltimento
8) controlli
9) inosservanza
10) aggiornamento.

Le disposizioni di seguito devono essere conosciute ed applicate dai soggetti autorizzati che accedono agli strumenti informatici aziendali e/o connessi al perseguimento di finalità aziendali.

1) Utilizzo del computer (fisso e portatile)

Il computer che l'utente ha ricevuto in dotazione è uno strumento di lavoro da utilizzarsi nel rispetto dei principi di correttezza e diligenza per perseguire finalità di tipo aziendale e/o previste dalla legge.

Il computer presenta caratteristiche hardware e software impostate dal Sistema informatico e che non possono essere modificate.

Le gestioni locali dei dati deve scomparire ed essere sostituita da gestione centralizzata su server.

Non è consentita l'installazione di programmi diversi da quelli autorizzati dal Sistema informatico il quale può altresì procedere alla rimozione di file o applicazioni che ritiene pericolosi per la sicurezza.

E' vietato l'uso di supporti removibili per la memorizzazione di dati particolari.

Durante l'uso del computer l'utente deve vigilare affinché i dati in esso contenuti non siano oggetto di accesso non autorizzato.

In pausa pranzo e nel caso di prolungata assenza dall'ufficio deve essere attivata la modalità "blocca computer".

Alla fine della giornata lavorativa è necessario spegnere completamente il computer e tutti gli asservimenti ad esso collegati.

Periodicamente è opportuno “pulire” il computer mediante la cancellazione di file superati o inutili.

Non è consentita la riproduzione o la duplicazione di programmi informatici ai sensi delle Legge n.128 del 21.05.2004 (interventi antipirateria).

L'utente è responsabile del computer portatile assegnatogli dall'Azienda e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo.

Ai portatili si applicano le stesse regole di utilizzo previste per i computer fissi.

II portatile deve essere presidiato direttamente oppure riposto in luogo sicuro.

L’utente non deve utilizzare abbonamenti internet privati per effettuare collegamenti alla rete.

2) Gestione della password

Per accedere alla rete è necessario utilizzare il proprio profilo personale come configurato e autorizzato dal Sistema informatico.

Il trattamento di dati personali con strumenti elettronici è consentito agli utenti dotati di credenziale di autenticazione (ad esempio password, smart card eccetera) segreta e esclusiva dell’utente stesso.

La password deve avere una verifica in due passaggi (conosciuta anche con il nome di autenticazione a due fattori), che aggiunge un ulteriore livello di sicurezza all’ account in quanto si esegue l'accesso fornendo un elemento noto (la tua password) e un elemento in possesso dell’utente (un codice).

L’utente deve creare una password priva di riferimenti banali (ad esempio è sconsigliato indicare il proprio nome, la propria data di nascita, il nome del coniuge eccetera)

L’utente deve modificare la password al primo utilizzo e, successivamente, almeno ogni sei mesi.

Nel caso di trattamento di dati personali e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.

L’utente autorizzato a trattare dati personali deve adottare le necessarie cautele per assicurare la segretezza e l’esclusività della password (ad esempio non scrivere la password su promemoria da appiccicarsi al computer né adottare procedure automatiche).

Nel caso in cui l’utente reputi che la password abbia perso la necessaria caratteristica di segretezza la stessa deve essere immediatamente sostituita previa comunicazione al Sistema informatico.

3) Utilizzo della rete aziendale e della rete esterna internet

L’accesso alla rete è consentito nel rispetto dei principi di correttezza e diligenza per perseguire finalità di tipo aziendale e/o previste dalla legge.

E’ vietato connettere in rete postazioni di lavoro se non in virtù di autorizzazione del Sistema informatico.

E’ vietata l’installazione non autorizzata di modem che sfruttino il sistema di comunicazione telefonico per l’accesso a banche dati esterne o interne all’azienda

In particolare l'utilizzo e l'accesso ad internet, attraverso la rete aziendale non è consentito per perseguire scopi privati e/o vietati dalla legge ma solo per ragioni di lavoro al fine di raggiungere obbiettivi di studio, ricerca e documentazione.

Non è permesso l'uso della rete internet per attività ludiche.

E' vietato scaricare programmi da siti internet se non previa autorizzazione del Sistema informatico.

E' vietata la partecipazione a forum, chat line, bacheche elettroniche non autorizzate.

Non è consentita la visione/memorizzazione di materiale di natura oltraggiosa, minacciosa, offensiva, oscena e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinioni e appartenenza politica.

L'Azienda si riserva la facoltà di porre limiti alla navigazione Internet escludendo siti non consoni allo svolgimento dell'attività lavorativa e/o comunque non affidabili, bloccando totalmente o parzialmente, in determinate fasce orarie, l'accesso a internet, ovvero bloccando l'accesso ad internet a determinati reparti/dipendenti/collaboratori qualora non necessario per fini lavorativi.

4) Uso della posta elettronica

L'abilitazione alla posta elettronica deve essere preceduta da regolare richiesta del Responsabile di funzione/unità organizzativa al Sistema informatico.

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

A ciascuna casella viene fornita una password di attivazione che l'utente avrà il compito di modificare al primo accesso alla stessa. Sarà completa responsabilità dell'utente la conservazione della password di accesso, della sua gestione e della sua modifica d intervalli periodici.

E' possibile consultare la posta elettronica aziendale utilizzando solo dispositivi mobili (BlackBerry o altri dispositivi) autorizzati da ASF SAN GIULIANO MILANESE.

Le comunicazioni in forma elettronica devono avvenire esclusivamente con l'utilizzo del sistema di posta elettronica di ASF SAN GIULIANO MILANESE.

Nel caso di mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da virus occorrerà cancellare i messaggi senza aprirli.

Nel caso di messaggi provenienti da mittenti conosciuti con allegati però sospetti (ad esempio file exe, scr, pif, bat, cmd), questi ultimi non devono essere aperti.

Non è consentito inviare a terzi/esterni all'azienda materiale di proprietà della ASF SAN GIULIANO MILANESE senza preventiva autorizzazione.

Nell'ipotesi di invio di allegati "pesanti" l'utente deve utilizzare un formato compresso (zip, jpg).

L'utente deve controllare i file in allegato di posta elettronica prima del loro utilizzo.

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

Periodicamente deve essere eseguita l'archiviazione dei messaggi obsoleti.

E' concesso l'uso della posta elettronica come mezzo di comunicazione personale a condizione che il tempo e i mezzi impiegati siano di entità trascurabile.

L’Azienda mette a disposizione del lavoratore apposite funzionalità di sistema che consentono di inviare automaticamente, in caso di assenze, messaggi di risposta contenenti le coordinate (anche telefoniche o anche elettroniche) di un altro soggetto o altre utili modalità di contatto. Si prescrive ai lavoratori di avvalersi di tale modalità, in caso di assenze.

In caso di eventuali assenze non programmate (ad es. per malattia o simili), l’Azienda, in presenza di improrogabili necessità legate all’attività lavorativa, ha la facoltà di fare in modo che la posta elettronica diretta al lavoratore assente venga dirottata, mediante personale appositamente incaricato (amministratore di sistema) su di un altro lavoratore (di norma il suo diretto responsabile), con avvertimento al mittente che il destinatario della sua mail è cambiato.

5) Protezione

L’utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale.

Ogni utente è tenuto a controllare la presenza e il regolare funzionamento del programma antivirus aziendale e consentire i periodici aggiornamenti dello stesso.

Nel caso che il programma antivirus rilevi la presenza di un virus l’utente dovrà sospendere ogni elaborazione in corso senza spegnere il computer e segnalare l'accaduto al Sistema informatico.

Ogni dispositivo magnetico di provenienza esterna all'azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo.

6) Salvataggio

L’utente deve provvedere ad effettuare il salvataggio dati, con frequenza giornaliera, sui supporti di rete o su supporto magnetico previa autorizzazione del Sistema Informatico.

Nel caso di salvataggio su supporto magnetico l’utente deve sostituire periodicamente gli stessi e provvedere alla loro conservazione in un luogo sicuro.

7) Smaltimento

Tutti i supporti contenenti dati riservati devono essere smaltiti in modo da evitare la divulgazione di informazioni riservate.

I supporti rimovibili contenenti dati particolari o dati giudiziari se non utilizzati devono essere distrutti o resi inutilizzabili.

Possono essere riutilizzati da altri soggetti se le informazioni precedentemente in essi contenute non sono intelligibili né tecnicamente in alcun modo ricostruibili.

8) Controlli

L’Azienda si riserva la facoltà di verificare a livello informatico, per finalità di sicurezza e tutela del proprio patrimonio, l'esistenza di un comportamento illecito del dipendente nell’uso degli strumenti elettronici, accesso a internet e uso della posta elettronica.

Le verifiche si svolgeranno nel rispetto della libertà, della segretezza delle comunicazioni e delle garanzie previste dallo Statuto dei lavoratori e del Regolamento 2016/679 del Parlamento Europeo e del Consiglio, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati .

In particolare, ferme restando le misure organizzative e tecniche adottate al fine di prevenire eventuali utilizzi impropri e distorti degli strumenti informatici (es. black-list, sistemi antivirus, sistemi di intrusion prevention ecc.), l'Azienda per una questione di sicurezza, provvede comunque a verificare gli accessi a internet in forma aggregata, analizzando i tempi di connessione senza indagare sui siti oggetto di accesso, in ottemperanza a quanto previsto dal Garante Privacy.

Nel caso in cui da queste verifiche emergano anomalie nel traffico dati o rischi per la sicurezza, l'Amministratore di sistema invierà al Responsabile dell'area coinvolta un avviso generalizzato richiamando gli utenti ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite all'interno del presente documento. Solo in fasi successive e nei casi di reiterata violazione delle procedure, l'Azienda restringerà il campo di intervento ed effettuerà controlli prolungati e costanti fino ad arrivare all'analisi dei singoli file di log.

A seguito delle verifiche informatiche potranno essere raccolti dati personali che saranno trattati in modo lecito e secondo correttezza, nel rispetto dei principi di pertinenza e non eccedenza della finalità di tutela della sicurezza e del patrimonio.

In particolare per quanto concerne il monitoraggio della posta elettronica l'Azienda non procede alla lettura e registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, se non nei limiti di quanto tecnicamente necessario per garantire il funzionamento del servizio *e-mail*.

Eventuali informazioni di natura sensibile potranno essere trattate dall'Azienda se necessario per far valere o difendere un diritto in sede giudiziaria.

9) Inosservanza delle disposizioni

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.

L'utente è considerato direttamente responsabile per un eventuale accesso illecito.

L'utente è considerato direttamente responsabile per l'appropriazione indebita del materiale cartaceo utilizzato per stampare i risultati della navigazione.

L'utente è considerato direttamente responsabile per il danneggiamento della rete aziendale a causa dei virus informatici introdottisi.

E' fatto salvo il diritto dell'Azienda di chiedere l'ulteriore risarcimento del danno.

10) Gestione dei data breach

L'art. 33 del GDPR impone al Titolare di notificare la violazione di dati al Garante Privacy entro 72 ore dal momento in cui ne viene a conoscenza, quindi nel momento in cui il titolare acquisisce consapevolezza dell'avvenuta infrazione dei dati.

E' dunque estremamente importante che il dipendente che sia incorso o che sia a conoscenza di una violazione di dati (quali una perdita accidentale dei dati o una violazione dei dati come conseguenza di un furto o di una sottrazione dolosa) informi immediatamente il Titolare della violazione.

A tal fine il dipendente dovrà informare il Responsabile della Protezione dei Dati, Dott.ssa Cristina Omini, Dott.ssa Cristina Omini, reperibile presso la sede di Via San Remo 3 – 20098 San Giuliano Milanese al seguente indirizzo e-mail: dpo@asfsangiuliano.it segnalando l'accadimento al fine da far scattare immediatamente l'obbligo di notifica.

Nel caso in cui occorra instaurare un'indagine più approfondita in merito alla verificazione di un incidente di sicurezza, il dipendente si impegna a collaborare con il Titolare.

11) Aggiornamento

Il presente Regolamento è soggetto a revisione con frequenza periodica e si inquadra nel più ampio obbligo di sicurezza che l'Azienda adempie al fine di proteggere i dati personali in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Al fine di scoprire e comunicare le possibili violazioni al sistema informatico è necessaria la collaborazione dell'utente nel segnalare ogni anomalia (ad esempio smarrimento o furto di informazioni, virus, violazioni di sicurezza).

In caso di violazione o perdita accidentale di dati, l'utente deve dare tempestiva comunicazione al Sistema informatico affinché possa procedere a segnalare la violazione al Garante della Privacy, entro 72 ore dal momento in cui ne è venuto a conoscenza come previsto dall'art.33 del Regolamento 2016/679 del Parlamento Europeo e del Consiglio, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati ed adotti le necessarie contromisure e per proporre altresì le integrazioni al presente Regolamento ritenute opportune.