Scuola dell'Infanzia
MOISO
Via Fratelli Moiso, 28 – 15011 Acqui Terme (AL)
☎ 0144/322928 – fax: 0144/352800 - scuolainfanziamoiso@gmail.com

Acqui Terme, 1° settembre 2021

Oggetto: designazione dell'Amministratore di sistema

Il Titolare dei trattamenti

Visto il Regolamento UE 679/16, che d'ora in poi nel presente documento sarà richiamato semplicemente come "Regolamento";
il Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 in G.U. n° 300 del 24 dicembre 2008 che d'ora in poi nel presente documento sarà richiamato semplicemente come "Provvedimento";

Premesso che
- Ai sensi dell'art. 28 del Regolamento nel presente atto, Titolare dei dati personali trattati da parte di questa Scuola è BUFFA Marina Silvia, di cui è Legale Rappresentante pro-tempore;
- L'art. 28 del Regolamento consente la facoltà di nominare uno o più Responsabili di tutti o parte dei trattamenti;
- L'art. 32 impone di adottare le misure di sicurezza disposte dal Regolamento;

considerato che
- L'art. 2 lettera a) del Provvedimento prescrive che la nomina degli amministratori deve avvenire previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza;
- **L'art. 2 lettera b) del Provvedimento prescrive che la designazione quale amministratore di sistema deve essere individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.**
- L'art. 2 lettera c) del Provvedimento prescrive che nel caso di servizi di amministrazione di sistema affidati in *outsourcing* il titolare deve conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

ritenuto che

in base alla valutazione del servizio di assistenza fino ad oggi prestato, alle referenze riscontrate mediante la conoscenza di analoghi contesti nei quali si è trovato ad operare, RIPANE Amedeo abbia adeguate capacità professionali, esperienza e affidabilità, tali da fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza,

determina

1) di designare **RIPANE Amedeo, amministratore di sistema** con il compito di sovrintendere alla gestione del sistema informatico in uso nella struttura organizzativa "segreteria" e nelle altre strutture, anche didattiche, qualora le misure da adottare riguardino apparati, impianti, parti di rete o dispositivi informatici di memorizzazione o elaborazione in comune
2) Di autorizzare l'Amministratore di sistema ad operare, anche per mezzo di collegamenti dall'esterno purché effettuati con modalità tali da non compromettere la sicurezza complessiva del sistema, sui sistemi e sugli archivi e sui documenti in essi contenuti anche in presenza di dati personali e sensibili riguardanti il personale, gli alunni e le loro famiglie limitando i trattamenti e le operazioni a quelli necessari al mantenimento in efficienza del sistema informatico.
3) Di definire i seguenti ambiti di competenza, che l'Amministratore, sottoscrivendo la presente determina, accetta:
   a) di organizzare la gestione dei computer e dei dispositivi elettronici che trattano dati personali e i relativi archivi elettronici in modo da garantire adeguata protezione dei dati, anche in relazione al loro grado di sensibilità e di delicatezza, nonché di garantirne la protezione da eventi che potrebbero danneggiare o far perdere documenti;
   b) di autorizzare gli accessi dei singoli incaricati limitandone la possibilità di operare sulla base del proprio mansionario secondo le indicazioni che verranno trasmesse dal Responsabile dei trattamenti;
   c) di supportare la segreteria circa l'utilizzo del programma applicativo (sia attuale che, in caso di cambiamento, di ogni applicativo che verrà adottato anche sulla base delle indicazioni ministeriali) definendo le possibilità di accesso dei diversi utenti in base alle specifiche mansioni ricoperte;

Scuola dell'Infanzia
MOISO
Via Fratelli Moiso, 28 – 15011 Acqui Terme (AL)
☎ 0144/322928 – fax: 0144/352800 - scuolainfanziamoiso@gmail.com

d) di prendere le misure opportune, organizzative e tecniche, per evitare accessi, intrusioni fisiche o tramite internet ai dati personali;
e) di organizzare un sistema di copia dei dati su supporti anche esterni al fine di poter recuperare un documento o un archivio eventualmente danneggiato o cancellato, di poter recuperare i documenti, i programmi, la configurazione del sistema in caso di sostituzione del server o di altro componente significativo;
f) di organizzare un sistema di verifica **con frequenza almeno semestrale** della funzionalità e della sicurezza complessiva del sistema informatico. della efficacia delle misure adottate e del loro funzionamento nonché del ruolo degli addetti interni eventualmente coinvolti nella attuazione delle misure di sicurezza adottate;
g) di adottare le soluzioni tecniche idonee a garantire il rispetto delle prescrizioni del Garante contenute nel provvedimento del 27 novembre 2008, e nei suoi eventuali aggiornamenti dei quali daremo ampia documentazione, riguardo alla tracciabilità delle operazioni effettuate dall'Amministratore di Sistema ed alla conservazione dei registri allo scopo prodotti;
h) <u>se il ruolo di amministratore viene affidato ad una società o ad un professionista esterno all'organizzazione scolastica</u> di descrivere dettagliatamente gli interventi che verranno eseguiti sui sistemi informatici mediante la compilazione di rapportini di intervento o di altri strumenti analoghi, dai quali si desuma: data dell'intervento, durata, tecnici che lo hanno effettuato, operazioni svolte, strumenti coinvolti (server, router, firewall, PC) o ogni altro dettaglio utile alla comprensione dell'intervento svolto.

4) Di ottenere dall'Amministratore designato, **se il soggetto destinatario della presente determina è una società**, l'elenco dettagliato dei tecnici che saranno autorizzati ad accedere ai nostri sistemi ed agli archivi in essi contenuti.
5) Di mettere a disposizione dell'Amministratore di Sistema la documentazione necessaria alla definizione delle misure di sicurezza e delle procedure operative nel totale rispetto delle prescrizioni normative attuali e di futura emanazione.
6) Di disporre che, venga riportato nella prossima revisione della lista di controllo degli adempimenti, a cura del Responsabile dei trattamenti, l'elenco degli amministratori di sistema nominati ai sensi della presente determina e dei tecnici segnalati ai sensi del punto 4).
7) Di consegnare copia della presente determina al soggetto indicato al punto 1) il quale sottoscrive per accettazione impegnandosi ad applicarne e rispettarne il contenuto.

Documenti a disposizione presso il Responsabile dei trattamenti:
- Regolamento UE 679/16
- Provvedimento 27 novembre 2008

Il titolare del trattamento

VIA F.lli MOISO, 28 - 15011 ACQUI TERME (AL) - Scuola dell'Infanzia MOISO

Per presa visione e accettazione

L'amministratore di Sistema

Data: 01/09/2021

Scuola dell'Infanzia
MOISO
Via Fratelli Moiso, 28 – 15011 Acqui Terme (AL)
☎ 0144/322928 – fax: 0144/352800 - scuolainfanziamoiso@gmail.com

REGOLAMENTO PER IL RISPETTO DELLA NORMATIVA IN TEMA DI TRATTAMENTO DEI DATI E MODALITA' OPERATIVE PER LA SICUREZZA DEL SISTEMA INFORMATICO.

AI SENSI
D.LGS. N° 196 DEL 30/06/2003
REGOLAMENTO UE 679/16

Allegato alla lettera di incarico di amministratore di sistema
articolo 29 e articolo 32 comma 4 Regolamento UE 679/16

INTRODUZIONE

Le informazioni sono un patrimonio aziendale di grande valore e, qualunque sia il modo di raccoglierle, memorizzarle, trasmetterle e conservarle, è essenziale mettere in atto tutte le precauzioni necessarie per salvaguardarne la riservatezza, l'integrità, e la disponibilità.

La normativa per la quale abbiamo redatto questo Regolamento riguarda nello specifico i dati personali, comuni e sensibili, ma la stessa attenzione deve essere adottata per tutti i dati e le informazioni che possiamo trovare nei nostri sistemi informatici e, più in generale, in tutta la nostra struttura.

Da tempo la Scuola dell'Infanzia MOISO ha deciso di agire sul fronte della Sicurezza Informatica adottando misure organizzative e tecniche che vadano oltre il formale rispetto delle previsioni normative ma che trovino, nella concretizzazione di effettivi benefici in termini di sicurezza e di efficienza, la loro ragione di essere.

Gestire le informazioni correttamente e con strumenti efficienti non vuole dire rendere difficoltoso il loro utilizzo ma garantire l'accesso ai dati e agli strumenti a quelle funzioni operative che ne abbiano necessità per svolgere le mansioni che vengono affidate loro. La corretta applicazione di questo principio in ogni fase del trattamento delle informazioni contribuisce alla costruzione dei un sistema di informazioni corretto, efficiente, utile, sicuro.

Un ruolo importante in questa costruzione lo ricoprono i tecnici informatici. Sulla loro correttezza e deontologia professionale, oltre che sulle loro capacità, facciamo affidamento.

Questo manuale, redatto con il contributo di diverse funzioni operative, vuole essere cose diverse:

- una guida pratica per sensibilizzare circa la necessità di trattare correttamente le informazioni che costituiscono il patrimonio informativo aziendale;
- una guida pratica per rispondere alle domande più comuni riguardanti la sicurezza informatica;
- una descrizione delle caratteristiche del sistema informatico in uso nella nostra struttura;
- una descrizione delle misure di sicurezza adottate e di come ogni incaricato abbia un ruolo nella loro applicazione;
- una descrizione dei comportamenti da tenere per ridurre al minimo i rischi insiti nei trattamenti di dati, personali e non, effettuati mediante gli strumenti elettronici.

Ma questo manuale assolve anche ad un altro compito, auspicato dal Garante per la protezione dei dati personali, quello di consentire al datore di lavoro di informare il dipendente circa le implicazioni che la tecnologia e l'uso degli strumenti in dotazione, PC, palmari, apparati per traffico dati, caselle di posta elettronica nominali, introducono nel rapporto fra datore di lavoro e dipendente che questi strumenti adopera.

Il rapporto fra datore di lavoro e dipendente: le implicazioni introdotte dalle nuove tecnologie
Il provvedimento del Garante del 23 novembre 2006 in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro riconosce al datore di lavoro, titolare dei trattamenti e delle risorse informatiche utilizzate, il **dovere** di garantire la sicurezza del patrimonio aziendale tecnico e informativo.

Per perseguire tale finalità il datore di lavoro ha il diritto di definire preventivamente le regole alle quali i propri incaricati devono attenersi, limitandone, se ne ravvede la necessità, la possibilità di operare sia attingendo alle risorse interne, sia nell'utilizzo delle risorse esterne (web o collegamenti ad altri sistemi).

L'applicazione di queste regole può avvenire con due diverse modalità:

a) formando il personale e lasciando ad esso la discrezionalità di applicare le indicazioni ricevute;
b) attivando sistemi di filtro preventivi attribuendo ad ogni unità operativa o ad ogni singolo incaricato i permessi e le risorse necessarie a svolgere le proprie mansioni.

Entrambe queste modalità comportano vantaggi e svantaggi. In alcuni casi bisognerà arrivare ad un bilanciamento delle due al fine di ottenere contemporaneamente sicurezza, riservatezza e possibilità operativa.

Nella prima modalità si otterrà la massima elasticità del sistema e l'operatore non incontrerà ostacoli nella sua azione ma il datore di lavoro sarà costretto ad attivare sistemi di tracciabilità delle operazioni eseguite dall'operatore non al fine di "spiarne" l'attività ma al fine di essere in grado, per ragioni di sicurezza, di ricostruire la causa di un ipotetico danno per potervi porre rimedio e fare sì che non si verifichi in futuro. Le azioni che un incaricato compie lasciano tracce nei registri informatici, i cosiddetti "log". L'analisi di questi log potrebbe far emergere situazioni particolari nelle quali l'incaricato si sia imbattuto.

Precisiamo che nessuna azione potrà essere adottata dal datore di lavoro a seguito della conoscenza delle informazioni ricavate dall'analisi dei log e che gli amministratori di sistema sono tenuti alla massima riservatezza, ma non si può negare che la conoscenza da parte di terzi sia possibile.

La seconda modalità limita, di fatto, la necessità di analizzare i "log", Quindi, sostiene il Garante, al fine di preservare la riservatezza dell'incaricato, **è auspicabile** che il datore di lavoro adotti quei sistemi procedurali, organizzativi e tecnici che, limitando preventivamente le possibili operazioni non strettamente necessarie allo svolgimento delle mansioni dell'incaricato, riducano la necessità che si debba ricorrere all'analisi dei log per valutare un evento informatico dannoso.

Resta, ed è giusto che sia così, la possibilità per il datore di lavoro, di tutelare il patrimonio aziendale attivando controlli mirati sia sull'attività già svolta che preventivi.
A tutela della riservatezza e della dignità dei soggetti coinvolti il Garante obbliga il datore di lavoro ad adottare procedure di informazione preventiva con le quali l'incaricato sia portato a conoscenza delle finalità e delle modalità dei controlli.

La diffusione di nuove tecnologie ha comportato l'aumento delle possibilità di accesso ai dati aziendali anche al di fuori dei luoghi di lavoro. La nostra organizzazione mette a disposizione ad alcune funzioni aziendali strumenti idonei a operare secondo queste modalità. In questi casi la corretta adozione delle misure di sicurezza diventa indispensabile al fine di ridurre il rischio che importanti informazioni contenute negli strumenti in dotazione vengano perse o vengano inopportunamente a conoscenza di terzi o diffuse.

In ultimo, la nostra organizzazione è tenuta al rispetto, fra le altre, delle norme relative alla tutela del diritto d'autore, sia in campo artistico che nelle opere d'ingegno.
Gli Amministratori di Sistema sono quindi tenuti ad utilizzare solo software acquistato e registrato o software in versione freeware o shareware solo se lo ritengono indispensabile. Nessun operatore dovrà essere in grado di installare software diversi da quelli previsti dagli Amministratori di Sistema.
La stessa regola dovrà riguardare la possibilità di scaricare da diverse fonti file protetti dal diritto d'autore (testi, immagini, file musicali, video) sui sistemi aziendali. Utilizzare queste tipologie di documenti informatici ci esporrebbe a pesanti sanzioni a risarcimento dei detentori dei diritti.

Ci aspettiamo la massima collaborazione nell'applicazione del contenuto del presente regolamento, certa che le sue finalità siano condivise da tutti coloro che sono chiamati ad applicarle.

Parte 1
LE LINEE GUIDA

PREMESSA

Fin dall'entrata in vigore del Decreto Legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), in materia di tutela dei Dati Personali (di seguito il "Codice"), **ora sostituito dal Regolamento UE 679/16** la nostra organizzazione è tenuta a conformarsi con il dettato normativo. Nel chiedere il rispetto di tali norme a tutti gli operatori, abbiamo predisposto le presenti linee guida al fine di sensibilizzare tutti gli incaricati e formarli in merito ai citati obblighi normativi, nonché al fine di formalizzare alcune prassi che ne facilitino il rispetto.

Ai fini del presente documento valgono le seguenti definizioni:

per "**Dati Personali**", qualunque informazione relativa a persona fisica, identificata o identificabile (ad esempio, Clienti, Fornitori, Dipendenti), anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

per "**Interessato**", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i Dati Personali o Sensibili (per esempio: Clienti, Fornitori, Dipendenti, Candidati, ecc.);

per "**Trattamento**", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici;

per "**Amministratori di Sistema**", i soggetti cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di basi di dati e di consentirne l'utilizzazione (ovvero, gli Incaricati autorizzati all'uso delle password di "*administrator*" dei sistemi operativi o di codici utente diversi ma parimenti autorizzati alle funzioni di amministrazione);

per "**Incaricati**", le persone fisiche autorizzate a compiere operazioni di trattamento (vedi "**Trattamento**") dal Titolare o dal Responsabile (ovvero, tutto il personale che abbia accesso a Dati Personali e, in quanto tale, individuato per iscritto come Incaricato da parte del Responsabile del trattamento competente per l'UO di riferimento).

per "**Dati Sensibili**", i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

per "**Comunicazione**", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione (forme di comunicazione sono: la posta, il telefax, l'e-mail);

per "**Diffusione**", il dare conoscenza dei Dati Personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione (per esempio: trasmissioni radiofoniche o televisive, stampa, pubblicazione su pagine WEB ad accesso non selezionato);

per "**Misure di Sicurezza**", il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza, previste dalla normativa vigente ed esplicitate in documentazione ufficiale della Scuola (Incarichi, Linee Guida, ecc.), che configurano il livello di protezione richiesto in relazione ai i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;

per "**Strumenti**", i mezzi elettronici o comunque automatizzati con cui si effettua il trattamento (elaboratori, supporti, apparecchi di telecomunicazioni, ecc.);

L'AMMINISTRATORE DI SISTEMA E GLI INCARICATI DELLA MANUTENZIONE

"Il Titolare, o il Responsabile competente, deve nominare uno o più Amministratori di sistema cui sia conferito il compito di sovrintendere alle risorse dei sistemi operativi degli elaboratori e, in generale, dei sistemi di basi dati, nonché i Gestori delle Password degli incaricati e degli utenti di rete."
"Il Titolare, o il Responsabile competente, deve individuare per iscritto gli Incaricati preposti alla manutenzione e gestione dei sistemi informativi aziendali."

Gli Amministratori di Sistema Responsabili sono i soggetti cui è conferito il compito di sovrintendere alle risorse dei sistemi operativi, degli elaboratori o dei sistemi di basi di dati e di consentirne l'utilizzazione in modo sicuro da parte degli Incaricati.
Sono considerati Amministratori di Sistema anche i dipendenti o collaboratori diretti dei Responsabili che svolgono le proprie mansioni su indicazione dei Responsabili stessi.
L'Amministratore di sistema è tenuto a non abusare delle proprie funzioni e mantenere la massima riservatezza in merito alle informazioni cui accede in relazione alle proprie mansioni e rispettare quanto stabilito dalle vigenti procedure di sicurezza.
Il citato Provvedimento Generale del Garante (G.U.300 del 24 dicembre 2008) prescrive che vengano portati a conoscenza degli operatori i nominativi degli amministratori di sistema che possono accedere agli strumenti informatici utilizzati dagli operatori nella struttura.
Il Titolare ha designato quale amministratore di sistema il Direttore dei Servizi Generali e Amministrativi.

Parte 2
RISERVATEZZA, STRUMENTI E DIRITTI

PREMESSE
Il presente Regolamento recepisce le indicazioni e le raccomandazioni fornite dal Garante per la protezione dei dati personali in occasione della pubblicazione del Provvedimento del 1 marzo 2007 (registro delle deliberazioni n. 13 del 1 marzo 2007, pubblicato sulla Gazzetta Ufficiale n. 58 del 10 marzo 2007) in merito alla regolamentazione dell'uso della posta elettronica ed internet sul luogo di lavoro al fine di individuare un punto di equilibrio tra i diritti del datore di lavoro e quelli del lavoratore e di definire le regole comportamentali per un utilizzo lecito e corretto della Posta Elettronica.

IL PROVVEDIMENTO GENERALE DEL GARANTE PER LA PRIVACY MARZO 2007
Il Provvedimento, il cui testo integrale è a disposizione sulla rete aziendale, ribadisce due concetti fondamentali apparentemente in contrasto fra di loro:

a) il diritto del lavoratore a che sia rispettata la propria dignità e la propria riservatezza
b) il dovere del datore di lavoro di adottare idonee misure di sicurezza al fine di ridurre al minimo i rischi di perdita dei dati contenuti sul sistema informatico, di accesso non autorizzato agli strumenti informatici, di trattamenti non conformi o potenzialmente pericolosi sia per il sistema informatico che per l'integrità dei dati in esso contenuti.

Al fine di poter assolvere il proprio dovere di vigilanza sull'integrità del sistema informatico e del patrimonio informativo in generale il datore di lavoro non può, soprattutto in fase di monitoraggio delle attività, ricavare informazioni relative al dipendente o collaboratore e a operazioni da lui effettuate, senza una serie di prerequisiti indispensabili.

Istruzioni
È senz'altro compito del datore di lavoro definire:

a) modalità di utilizzo delle risorse informatiche;
b) limiti all'utilizzo delle risorse informatiche;
c) margini discrezionali per consentire o negare l'utilizzo degli strumenti per finalità non direttamente collegate alle mansioni affidate al dipendente o collaboratore.

L'insieme delle misure di sicurezza e delle pratiche operative adottate deve essere portato a conoscenza del dipendente o collaboratore; questi è tenuto ad applicare quanto stabilito dal datore di lavoro collaborando per quello che il per il suo ruolo è stato previsto.

Limitazioni
Quando il solo impartire istruzioni operative non si rivelasse sufficiente a limitare un uso non corretto degli strumenti elettronici il datore di lavoro può adottare quegli accorgimenti tecnici che limitino la discrezionalità del dipendente o collaboratore impedendo alcune operazioni o consentendone un numero limitato. Questa soluzione è caldeggiata dal garante stesso con la motivazione che vengono in questo modo limitate le occasioni nelle quali si concretizzi la necessità di effettuare controlli e monitoraggi sulle attività di un operatore.

Controlli
Adottando misure di sicurezza e procedure operative efficaci, inserendo nel sistema informatico strumenti che governino i margini di operatività degli operatori, si riducono al minimo le necessità di analizzare nel dettaglio le attività degli operatori. Tuttavia questa necessità può sussistere.
I controlli, per essere validi, devono rispettare il criterio di gradualità e di pertinenza o non eccedenza. Il garante non ammette controlli "a tappeto", cioè prolungati, indiscriminati e costanti.
La possibilità di accedere alla posta elettronica contenuta nelle caselle in dotazione al dipendente o collaboratore deve essere definita in relazione alle possibilità operative concesse all'operatore stesso. La possibilità, o meno, di utilizzare la posta per comunicazioni personali deve essere definita e portata a conoscenza del dipendente o collaboratore nel Regolamento.
Nei prossimi paragrafi vengono quindi portate a conoscenza degli operatori le modalità di utilizzo della navigazione Internet, dell'utilizzo della posta elettronica e delle possibilità di accesso e di controllo da parte delle funzioni aziendali preposte.

REGOLAMENTO PER L'UTILIZZO DELLA POSTA ELETTRONICA

AMBITO DI APPLICAZIONE

La presente procedura si applica nell'ambito dell'utilizzo della Posta Elettronica aziendale per lo svolgimento delle proprie mansioni lavorative.

RESPONSABILITÀ

L'utilizzo della posta elettronica aziendale è fornito al personale a beneficio dell'intera organizzazione, dei clienti, dei fornitori e di tutti i soggetti con cui l'impresa intrattiene rapporti di comunicazione.

Tale possibilità, infatti, consente di comunicare velocemente incrementando così la propria produttività.

Il personale ha la responsabilità di salvaguardare e migliorare l'immagine pubblica dell'organizzazione e di utilizzare la posta elettronica per finalità legittime ed etiche, in stretta connessione allo svolgimento delle proprie mansioni.

Tutti gli utenti del servizio di Posta Elettronica (Responsabili, Incaricati o Utenti di rete) sono responsabili dell'applicazione rigorosa del presente Regolamento. L'amministratore di sistema ha l'obbligo di vigilare, nel rispetto dell'articolo 4 della L. 20 maggio 1970, n. 300 (Statuto dei lavoratori), sulla corretta applicazione della presente procedura da parte di tutto il personale dell'organizzazione, evidenziando le eventuali criticità rispetto a quanto disposto e proponendo al Responsabile dei trattamenti le soluzioni ritenute più idonee data la struttura dell'organizzazione.

MODALITÀ OPERATIVE

In primo luogo si premette che tutte le informazioni archiviate negli elaboratori (inclusi documenti, altri file, messaggi di posta elettronica e le registrazioni dei messaggi di posta vocale) sono di proprietà della struttura.

Ciò vale anche per la posta elettronica di tutti gli account dei domini sopra elencati (sia nominativi, es. nome.cognome@azienda.it, che di funzione, es. segreteria@azienda.it)

Gli Utenti dei servizi di posta elettronica devono essere consapevoli che tutte le comunicazioni inviate o ricevute mediante i sistemi di posta elettronica aziendali per finalità di lavoro devono quindi essere considerate informazioni di carattere non riservato nei confronti dell'imprenditore datore di lavoro.

Ogni ulteriore informazione, materiale, comunicazione creata, spedita o recuperata attraverso la rete Internet per finalità estranee a quelle di lavoro è da ritenersi abusiva ai sensi dell'articolo 11 del Codice Privacy, in quanto eccedente e non pertinente alle finalità del trattamento affidate agli Incaricati.

L'attribuzione ad un utente di uno o più indirizzi di posta, personale (qualsiasi combinazione di nome e cognome) o identificativo della funzione e del ruolo all'interno dell'organizzazione (amministrazione, marketing, direzione) è autorizzata per un uso esclusivamente professionale.
La Scuola, nel caso di cessazione del rapporto di lavoro o di assenze prolungate (ad esempio, per malattia o maternità) del lavoratore, si riserva il diritto di trattenere copia dei messaggi e di potervi accedere, per garanzie di continuità dei rapporti con i terzi, ovvero di accertamento preventivo o difensivo di fatti illeciti.
Le modalità di gestione dei messaggi che verranno indirizzati alla casella di posta nominale di un utente che abbia cessato il rapporto di collaborazione o che rimanga assente per un tempo prolungato verrà concordata fra il dipendente o collaboratore stesso, il suo responsabile di funzione e l'amministratore di sistema della struttura di riferimento. I termini dell'accordo saranno accettati e sottoscritti dal dipendente o collaboratore e applicati dall'amministratore di sistema.

L'utilizzo della casella di posta è vincolato alla immissione delle credenziali di autenticazione fornite dalla struttura IT dell'organizzazione. Tali credenziali possono essere preimpostate nell'applicativo fornito sul PC in dotazione o nel dispositivo portatile autorizzato.

L'eventuale utilizzo di procedure webmail autorizzate da Personal Computer al di fuori della struttura aziendale (internet point, casa) non dovrà prevedere la memorizzazione della password così da non permettere l'accesso ad altri utilizzatori degli stessi dispositivi.

Le credenziali fornite non possono essere cedute, o comunicate, a terzi e devono essere conservate applicando le attenzioni previste per ogni altro sistema di accesso ricevuto in dotazione.

Gli Utenti dei servizi di posta elettronica sono tenuti ad avvertire l'amministratore di sistema della struttura di riferimento nel caso ipotizzino che le proprie credenziali possano essere state usate da terzi.

Gli Utenti dei servizi di posta elettronica devono utilizzare i sistemi aziendali esclusivamente per ragioni professionali.
È consentito un limitato uso personale della posta elettronica purché non in contrasto con le disposizioni del presente regolamento e con lo svolgimento delle mansioni assegnate. Il dipendente o collaboratore, ricevendo il regolamento, viene portato a conoscenza che gli amministratori di sistema hanno accesso, nei limiti e per le finalità in esso dichiarate, agli archivi di posta.

Gli Utenti dei servizi di posta elettronica non possono utilizzare i sistemi aziendali per creare o trasmettere materiale con contenuti sessuali espliciti, denigratori, diffamatori, osceni od offensivi, quali, a titolo esemplificativo, insulti, epiteti ovvero qualsiasi altro contenuto o testo che possa essere considerato una molestia ovvero una discriminazione fondata sull'origine razziale, il colore della pelle, la nazionalità, il sesso, preferenze sessuali, età, infermità fisiche o psichiche, stato di salute, stato civile rispetto al matrimonio, convinzioni politiche o religiose.

Gli Utenti dei servizi di posta elettronica non possono utilizzare i sistemi aziendali per sollecitare o fare proseliti per finalità commerciali, di propaganda in favore di organizzazioni esterne, catene di lettere, ovvero per altre finalità estranee all'attività aziendale.

Gli Utenti dei servizi di posta elettronica devono utilizzare i sistemi aziendali esclusivamente per condurre affari aziendali ufficiali nonché per corrispondere comunicazioni comunque correlate agli affari condotti dall'organizzazione.

Gli Utenti dei servizi di posta elettronica non devono tentare di rappresentare la posizione dell'organizzazione, mediante l'uso di sistemi di posta elettronica aziendali, su qualsiasi questione di carattere pubblico attraverso forum di discussione, salvo per l'esecuzione di attività di natura professionale, e devono porre in essere ogni sforzo per salvaguardare l'immagine pubblica dell'organizzazione. Gli Utenti dei servizi di posta elettronica devono vigilare al fine di evitare la rivelazione attraverso e-mail, news-group o forum pubblici di informazioni confidenziali.

Gli Utenti dei servizi di posta elettronica non possono utilizzare i sistemi aziendali per scopi personali, di carriera, o di profitto individuale, ovvero per sollecitare un affare estraneo all'attività dell'organizzazione.

Gli Utenti dei servizi di posta elettronica sono responsabili in via esclusiva del contenuto di messaggi, file di testo, immagini, file audio da essi pubblicati o trasmessi attraverso i sistemi di posta elettronica aziendali per finalità non strettamente correlate alla mansione assegnata.

In ogni caso gli Utenti dei servizi di posta elettronica non possono utilizzare i sistemi aziendali per inviare o ricevere materiali protetti dal diritto d'autore, segreti commerciali, informazioni finanziarie proprietarie, o altro materiale appartenente ad altre organizzazioni, salvo per l'esecuzione di attività di natura professionale.

La mancata osservanza del diritto d'autore ovvero di accordi di licenza può condurre ad azioni disciplinari dell'organizzazione ovvero ad azioni legali dei legittimi titolari del diritto d'autore nei confronti di si è reso responsabile di tali atti.

Gli Utenti dei servizi di posta elettronica, in considerazione degli obblighi e dei doveri precedentemente descritti, possono accedere, nei limiti e secondo le modalità descritte nel successivo "Regolamento per l'utilizzo di Internet", alla propria casella di posta elettronica personale mediante l'utilizzo di procedure di webmail per l'invio e il ricevimento di messaggi di posta elettronica di natura strettamente personale.

È vietato, salvo autorizzazione del Responsabile dei trattamenti su richiesta motivata da parte dell'utente o del responsabile di funzione approvata dall'amministratore di sistema della struttura di riferimento, l'utilizzo di applicativi per la gestione della posta elettronica diversi da quello adottato dalla struttura IT dell'organizzazione.

In caso di assenza preventivata (ad es., per ferie o attività di lavoro fuori sede) gli Utenti dei servizi di posta elettronica dovranno impostare il proprio programma in modo che possa inviare automaticamente messaggi di risposta contenenti le "coordinate" (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura. Le modalità di impostazione del sistema di posta elettronica secondo quanto descritto sono pubblicate sulla intranet aziendale.
Altre modalità di gestione dei messaggi in caso di assenza (inoltro ad altro indirizzo, nomina di un fiduciario che possa accedere alla casella di posta o ricevere in copia i messaggi) dovranno essere concordate con l'amministratore di sistema della struttura di riferimento.

In caso di eventuali assenze non programmate (ad es., per malattia), qualora il lavoratore non possa attivare la procedura descritta (anche avvalendosi di servizi webmail), il Titolare del trattamento, perdurando l'assenza oltre un determinato limite temporale, può disporre, lecitamente, mediante l'azione degli Amministratori di Sistema, l'attivazione di un analogo accorgimento, avvertendo gli interessati.

In previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, l'utente potrà delegare, anche preventivamente, un collega (cosiddetto "fiduciario") a verificare il contenuto di messaggi e a inoltrare al Titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Il Fiduciario o il Titolare provvederanno a verbalizzare tale attività e ad informare il lavoratore interessato alla prima occasione utile.

Infine, i messaggi di posta elettronica dovranno contenere un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi, precisando se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente.

L'Amministratore di sistema precisa, in accordo con i propri operatori, che le caselle di posta elettronica utilizzate, sia generiche (es. info, amministrazione) che nominali (nome.cognome, n.cognome) non devono essere utilizzate per messaggi di natura personale o riservata in quanto i messaggi ricevuti o inviati possono essere analizzati dalle funzioni aziendali a ciò preposte per ragioni di sicurezza. In caso di assenza prolungata di un operatore i messaggi a lui indirizzati vengono letti da altre funzioni aziendali. In caso sia necessario attivare canali di comunicazione riservati si prega di contattare direttamente l'operatore interessato.
Il testo è pubblicato sulla Intranet aziendale e richiedibile al responsabile.

Gli Utenti dei servizi di posta elettronica che abbiano notizia di una qualsiasi violazione della presente procedura sono tenuti a darne comunicazione al proprio Responsabile. Gli Utenti dei servizi di posta elettronica che contravvengano alla presente procedura ovvero utilizzano l'utenza di posta elettronica aziendale per scopi impropri sono soggetti a sanzioni secondo quanto previsto dal contratto di lavoro di riferimento e/o da quanto previsto dalle vigenti normative e/o da regolamenti interni.

REGOLAMENTO PER L'UTILIZZO DELLA RETE INTERNET

OBIETTIVO
Il presente Regolamento si pone l'obiettivo di fornire le regole comportamentali per un utilizzo lecito e corretto della rete Internet.

AMBITO DI APPLICAZIONE
Il presente Regolamento si applica nell'ambito dell'utilizzo della rete Internet sia per lo svolgimento delle proprie mansioni lavorative sia per il limitato e consentito uso personale di tale strumento di lavoro.

L'accettazione e la stretta osservanza del presente Regolamento è condizione essenziale per ottenere l'attribuzione in uso del servizio di accesso a Internet mediante IP pubblici attribuiti alla responsabilità dell'ente.

RESPONSABILITÀ
L'accesso alla rete Internet è stato fornito al personale dell'organizzazione a beneficio dell'intera organizzazione e dei processi aziendali. Tale possibilità consente al personale di usufruire di risorse informative sparse in tutto il mondo e di incrementare così la propria produttività.

Il personale ha la responsabilità di salvaguardare e migliorare l'immagine pubblica dell'organizzazione, e di utilizzare la rete Internet per finalità legittime, etiche e strettamente necessarie allo svolgimento delle mansioni lavorative. Al fine di assicurare che tutti i responsabili, dipendenti/utenti di rete siano utenti responsabili della rete Internet, utenti produttivi e attenti alla salvaguardia dell'immagine pubblica dell'organizzazione, è stata predisposto il presente Regolamento relativo all'utilizzo della rete Internet e/o degli accessi alla stessa attraverso la rete aziendale durante l'orario di lavoro. Pertanto, tutti gli utenti (Responsabili, Incaricati o Utenti di rete) sono responsabili dell'applicazione rigorosa del presente Regolamento. Gli amministratori di sistema della struttura di riferimento hanno l'obbligo di vigilare, nel rispetto dell'articolo 4 della L. 20 maggio 1970, n. 300 (Statuto dei lavoratori), sul rispetto della presente procedura da parte di tutto il personale dell'organizzazione.

MODALITÀ OPERATIVE
Gli utenti abilitati all'utilizzo della rete che hanno accesso alla rete Internet devono utilizzare questo strumento esclusivamente per ragioni professionali.

È consentito l'uso a fini personali esclusivamente per l'accesso alla propria casella privata di posta tramite il web (cosiddette webmail), con periodicità tale da non inficiare l'attività lavorativa.

Le prescrizioni – riportare in questo Regolamento – sui contenuti ed i materiali veicolati tramite rete Internet devono essere rispettate anche con riferimento alla web mail privata, poiché vengono utilizzate risorse aziendali.

Gli utenti abilitati all'utilizzo della rete possono utilizzare le normali risorse web e ftp della rete Internet esclusivamente per condurre affari aziendali ufficiali, ottenere pareri tecnici o analitici, per accedere ad informazioni relative alle attività dell'organizzazione o comunque correlate agli affari condotti dall'organizzazione. Non è consentito l'utilizzo di piattaforme di scambio peer to peer o di download continuativi, salvo esplicita autorizzazione del responsabile di funzione per comprovata necessità di servizio. In questo caso la procedura verrà impostata dall'Amministratore di Sistema competente per la struttura.

Gli utenti abilitati all'utilizzo della rete non devono tentare di rappresentare la posizione dell'organizzazione su qualsiasi questione di carattere pubblico attraverso forum di discussione, salvo per l'esecuzione di attività di natura professionale e devono porre in essere ogni sforzo per salvaguardare l'immagine pubblica dell'organizzazione.

Gli utenti abilitati all'utilizzo della rete devono vigilare al fine di evitare la rivelazione di informazioni confidenziali attraverso e-mail, news-group o forum pubblici.

Gli utenti abilitati all'utilizzo della rete, al fine di evitare la propagazione di virus per elaboratori attraverso i sistemi aziendali, non possono effettuare il download di alcun software dalla rete Internet senza specifica autorizzazione da parte dell'Amministratore di Sistema. Dove sia tecnicamente possibile e non in conflitto con il normale utilizzo della risorsa informatica in dotazione questa funzione verrà disattivata dall'Amministratore di Sistema. Tutti i

download di software dovranno essere approvati e materialmente compiuti dagli Amministratori di Sistema che provvederanno poi alla distribuzione e all'installazione, se prevista.

Gli utenti abilitati all'utilizzo della rete possono accedere alla rete Internet mediante la rete aziendale durante l'orario di lavoro esclusivamente per attività nell'interesse dell'organizzazione e, sporadicamente, ad uso personale con i limiti riportati nella presente procedura.

Gli utenti abilitati all'utilizzo della rete non possono utilizzare la rete Internet per scopi personali, di carriera, o di profitto individuale, ovvero per sollecitare un affare estraneo all'attività dell'organizzazione.

Gli utenti abilitati all'utilizzo della rete sono responsabili in via esclusiva del contenuto di messaggi, file di testo, immagini, file audio da essi pubblicati o trasmessi attraverso la rete Internet per finalità non strettamente correlate alla mansione assegnata.

Gli utenti abilitati all'utilizzo della rete non possono utilizzare Internet per immettere in Rete (upload) ovvero ricevere (download) materiali protetti dal diritto d'autore, segreti commerciali, informazioni finanziarie proprietarie o altro materiale appartenente ad organizzazioni diverse dall'organizzazione, salvo per l'esecuzione di attività legittime di natura professionale. La mancata osservanza del diritto d'autore ovvero di accordi di licenza può condurre ad azioni disciplinari dell'organizzazione ovvero ad azioni legali dei legittimi titolari del diritto d'autore.

Gli utenti abilitati all'utilizzo della rete non possono utilizzare la rete Internet per creare o trasmettere materiale con contenuti sessuali espliciti, denigratori, diffamatori, osceni od offensivi, quali, a titolo esemplificativo, denigrazioni, epiteti ovvero qualsiasi altro contenuto o testo che possa essere considerato una molestia ovvero una discriminazione fondata sull'origine razziale, il colore della pelle, la nazionalità, il sesso, preferenze sessuali, età, infermità fisiche o psichiche, stato di salute, stato civile rispetto al matrimonio, convinzioni politiche o religiose.

Gli utenti abilitati all'utilizzo della rete non possono utilizzare la rete Internet per sollecitare o fare proseliti per finalità commerciali, a beneficio di organizzazioni esterne, per catene di lettere, ovvero per altre finalità estranee all'attività dell'organizzazione.

Gli utenti abilitati all'utilizzo della rete devono essere consapevoli che tutte le comunicazioni create, spedite o recuperate dalla rete Internet per finalità di lavoro sono di proprietà dell'organizzazione e devono essere considerate informazioni di carattere pubblico.

Si ricorda che ogni informazione, materiale, comunicazione creata, spedita o recuperata attraverso la rete Internet per finalità estranee a quelle di lavoro è da ritenersi abusiva ai sensi del suddetto articolo 11 in quanto eccedente e non pertinente alle finalità del trattamento affidate agli Incaricati.

Attraverso la rete Internet è possibile accedere a siti che richiedono il versamento di quote di sottoscrizione o di utilizzo al fine di accedere alle informazioni disponibili sul sito. Gli Incaricati e gli Utenti di rete devono inoltrare al proprio Responsabile le richieste per l'approvazione di tali versamenti.

Gli utenti abilitati all'utilizzo della rete che abbiano notizia di una qualsiasi violazione della presente procedura è tenuto a darne comunicazione all'Amministratore di Sistema competente o al responsabile dei trattamenti.

Gli utenti abilitati all'utilizzo della rete che contravvengano alla presente procedura ovvero utilizzano l'accesso alla rete Internet per scopi impropri sono soggetti a sanzioni secondo quanto previsto dal contratto di lavoro di riferimento e/o da quanto previsto dalle vigenti normative e/o da regolamenti interni.

Parte 3
STRUMENTI E MODALITÀ OPERATIVE

INTRODUZIONE

Questa sezione intende formalizzare alcune linee guida per garantire il rispetto della vigente normativa in materia di riservatezza dei dati personali e la sicurezza dei sistemi informativi aziendali rispetto ai rischi di distruzione o perdita delle informazioni, accesso non autorizzato e trattamento non consentito.

Conformare il proprio comportamento a quanto di seguito indicato contribuirà al raggiungimento degli obiettivi della sicurezza, riassumibili nei tre aspetti distinti:

Disponibilità: ovvero, garantire l'accesso alle informazioni e ai servizi di rete da parte del personale incaricato in relazione alle esigenze lavorative;

Riservatezza: ovvero, garantire la prevenzione di accessi abusivi o non autorizzati alle informazioni, ai servizi e ai sistemi;

Integrità: ovvero, garantire che le informazioni non siano state alterate da incidenti o abusi.

Il raggiungimento di questi obiettivi richiede non solo l'utilizzo di appropriati strumenti tecnologici, ma anche gli opportuni meccanismi organizzativi; infatti, le misure tecniche, per quanto sofisticate, non saranno efficienti se non utilizzate propriamente.

In particolare, le precauzioni di tipo tecnico/informatico possono proteggere le informazioni durante il loro transito attraverso i sistemi ed anche quando queste sono registrate su un disco fisso di un elaboratore; ma nel momento in cui esse raggiungono l'utente incaricato, la loro protezione dipende esclusivamente dall'operato di quest'ultimo e nessuno strumento tecnologico può sostituirsi al suo senso di responsabilità e al rispetto di alcune semplici norme di comportamento.

LINEE GUIDA PER LA SICUREZZA

PROTEZIONE DELLA PROPRIA POSTAZIONE DI LAVORO

Riporre un documento sul quale sono contenuti dati personali o bloccare un terminale per mezzo del quale si accede a documenti e archivi, esclude la possibilità che terzi non incaricati vengano a conoscenza di informazioni anche solo frequentando gli uffici (visitatori o impresa di pulizie).
Nella nostra struttura gli uffici vengono puliti da una impresa esterna alla quale sono state trasmesse severe regole alle quali gli operatori dovranno attenersi scrupolosamente; tuttavia sarà essenziale che da parte degli incaricati ai trattamenti venga applicato il contenuto della presente sezione per evitare che il contenuto delle scrivanie possa inavvertitamente essere spostato, cestinato, consultato, smarrito o che i terminali possano essere utilizzati.

La norma prevede che l'accesso agli archivi, o ai documenti, contenenti dati sensibili e/o giudiziari sia permesso esclusivamente agli incaricati autorizzati. Riporre la documentazione utilizzata, chiudere, in assenza di almeno un incaricato autorizzato, se previsto, l'ufficio o almeno il dispositivo di conservazione sono quindi misure indispensabili in presenza di queste tipologie di dati personali. Tuttavia si ritiene necessario applicare queste modalità operative anche in presenza di soli dati comuni (documenti, elenchi, rubriche, agende).

Ogni operatore al quale viene assegnata una credenziale di accesso al sistema informatico ha a disposizione, di norma, una postazione operativa esclusiva composta da scrivania, cassettiera, dispositivi diversi per la conservazione di documenti. Fanno eccezione, a titolo esemplificativo:
- le postazioni operative utilizzate a rotazione da più personale;
- le postazioni di accesso a sistemi di rilevazione della produzione o tecnici.

Ogni operatore ha la responsabilità di applicare alla propria postazione le misure descritte in questa sezione al fine di non rendere accessibili i dati di propria competenza in caso di assenza, anche temporanea e di segnalare al Responsabile dei trattamenti situazioni logistiche che non ne consentano la piena applicazione.

CONSERVAZIONE DEI SUPPORTI (CD ROM, DISCHETTI, MEMORIE FLASH O FISICHE, COPIE CARTACEE, FASCICOLI, ECC.) IN UN LUOGO SICURO

Per quanto concerne i supporti (CD Rom, dischetti, memorie flash o fisiche, copie cartacee, fascicoli, ecc) che contengono dati personali, si applicano gli stessi criteri di attenzione e protezione descritti al precedente punto in tema di accesso ai locali e agli archivi. Per tali supporti esiste l'ulteriore pericolo che il loro smarrimento (che può anche essere dovuto a un furto) possa passare più facilmente inosservato. Pertanto, salvo il caso in cui l'incaricato sia certo che i supporti contengano solamente dati pubblici o conoscibili da chiunque, anche tali supporti dovranno essere riposti in un contenitore o cassetto munito di serratura non appena ne sia terminato l'utilizzo (per il caso di copie cartacee, le stesse dovranno essere riposte nell'archivio di provenienza).

Naturalmente, maggior attenzione dovrà essere posta per quei particolari tipi di dati denominati "sensibili e/o giudiziari" (stato di salute, vita sessuale, adesione o opinioni religiose, politiche o sindacali, origini razziali o etniche, dati provenienti dal casellario giudiziale, ecc.). Per tali ultimi dati e per dati di altra natura (anagrafici, economici, ecc.) ma di particolare importanza o riservatezza, in caso di trattamento informatico si raccomanda il salvataggio nelle apposite directory di rete ad accesso selezionato.

Non è consentita la copia degli archivi informatici su supporti rimovibili se non per operazioni autorizzate dagli Amministratori di Sistema. Qualora sia necessario il salvataggio su supporti rimovibili quest'ultimi dovranno essere custoditi dall'incaricato con le medesime modalità previste per altre tipologie di supporto, ad esempio cartacei. Se tecnicamente possibile il contenuto presente sul supporto dovrà essere protetto mediante password di apertura, mediante chiavi di cifratura o altri sistemi parimenti efficaci. Questi sistemi verranno forniti su richiesta dagli Amministratori di Sistema. Lo smarrimento o il guasto di un supporto affidato ad un incaricato dovrà essere da questi immediatamente segnalato ad un Amministratore di Sistema o al Responsabile dei trattamenti.

Il riutilizzo di un supporto magnetico od ottico è consentito a condizione che i dati in esso precedentemente contenuti siano irrecuperabili. Per garantire il rispetto di tale principio è quindi necessario procedere alla formattazione del supporto prima del riutilizzo dello stesso; alternativamente il supporto dovrà essere distrutto, affinché i dati in esso contenuti risultino essere irrecuperabili.

Le riproduzioni di documenti cartacei contenenti dati sensibili e/o informazioni relative al trattamento di dati personali devono essere conservati e custoditi con le medesime modalità previste per i documenti originali. Non è consentito riutilizzare il retro di fotocopie sul cui fronte siano impresse informazioni o dati personali.

UTILIZZO DI STAMPANTI, FOTOCOPIATRICI E FAX

Le stampanti, le fotocopiatrici e i fax/telefax sono beni aziendali e devono essere utilizzati dal personale esclusivamente per attività di carattere lavorativo e non per scopi di natura personale.

Per quanto concerne l'utilizzo delle stampanti, gli Incaricati devono stampare tutte le informazioni di natura sensibile o riservata esclusivamente su stampanti presenti all'interno dei propri uffici o in uffici i cui gli Incaricati siano autorizzati al trattamento dei medesimi dati assicurandosi di non lasciare incustoditi i documenti sulla stampante.
Relativamente alla stampa di documentazione contenente altri dati personali è opportuno che essa venga effettuata all'interno degli uffici preposti al trattamento. Qualora si debba ricorrere all' utilizzo di stampanti di rete ubicate in corridoi o locali di comune utilizzo, gli incaricati devono provvedere al tempestivo ritiro dei documenti.

Gli Incaricati che si accorgano di aver commesso un errore nella stampa devono procedere all'annullamento. Gli Incaricati che non siano riusciti ad annullare la stampa e si accorgano, al momento del ritiro della stampa, di errori che rendono inutilizzabili i documenti, devono provvedere alla distruzione dei medesimi nei propri uffici.

Per quanto concerne l'utilizzo delle fotocopiatrici gli Incaricati devono effettuare copie dei documenti nel numero strettamente necessario.

Le copie possono essere consegnate solo ad Incaricati preposti a trattare la determinata tipologia di dati contenuta nei documenti; qualora si effettuino copie di documenti che contengono dati sensibili e/o giudiziari o altri dati di natura riservata ma non sia assolutamente necessaria la conoscenza di questi, l'Incaricato deve renderli illeggibili prima di porre il documento nella fotocopiatrice.

Qualora l'Incaricato effettui copie di documenti contenenti dati sensibili e/o giudiziari o altri dati di natura riservata, non deve allontanarsi dalla macchina durante la copiatura, per evitare che Incaricati non autorizzati entrino in contatto con i dati.

Le copie ottenute devono, in ogni caso, essere sottoposte alle stesse misure di sicurezza dei documenti originali da cui sono state tratte.

per quanto concerne l'utilizzo di fax/telefax, gli Incaricati devono garantire, nella fase di *invio* di documenti contenenti dati personali, dati sensibili e/o giudiziari e altri dati di natura riservata, la massima riservatezza delle informazioni.
L'Incaricato deve riportare in ufficio sia il documento inviato sia il "rapporto di trasmissione".

Nella fase di *ricezione di* fax contenenti dati personali, dati sensibili e/o giudiziari e altri dati di natura riservata, gli Incaricati preposti alla gestione dei fax devono conservarli avvisando personalmente, telefonicamente o via e-mail interna, i destinatari dei documenti. Gli Incaricati destinatari dei documenti devono presentarsi personalmente al ritiro dei fax ricevuti. Nel caso di fax erroneamente indirizzati, gli Incaricati devono trattare tali documenti con la massima riservatezza in quanto potrebbero contenere dati personali o informazioni riservate appartenenti a terzi soggetti. Tali Incaricati non devono rispondere via fax al numero mittente, bensì devono verificare la presenza sul documento ricevuto di un numero telefonico da contattare per avvisare dell'erroneo invio. Soltanto dopo aver contattato il mittente o il destinatario del fax potranno eliminare definitivamente il documento ricevuto, utilizzando un dispositivo distruggi – documenti.

FASI DEL TRATTAMENTO DI DATI PERSONALI

Nel caso di trattamenti informatici di dati personali:

- cambiare la password di accesso ai sistemi nel rispetto delle modalità previste dalla normativa;
- non lasciare visualizzati sullo schermo dati personali in propria assenza (operazione di blocco del terminale mediante la pressione contemporanea dei tasti CTRL + ALT + CANC + INVIO);
- cancellare sempre tutti i dati residui presenti nell'elaboratore quando non più utilizzati;
- informare subito il responsabile del trattamento se si evidenzia un accesso a dati non di vostra competenza;
- tenere sotto controllo l'accesso fisico all'elaboratore e consentire l'eventuale utilizzo solo ad altri incaricati preposti al trattamento;
- accertare che vengano eliminate o distrutte in modo sicuro le cartucce delle stampanti a nastro (FAX) o laser, gli stampati dei computer, i dischetti non utilizzati e ogni altro oggetto o supporto informatico utilizzato per archiviare dati personali e/o sensibili, (prestare anche attenzione a cancellare i dati archiviati in aree di memoria del computer ad es. cestino di Windows).

Nel caso di comunicazioni di dati personali:

- se vengono richiesti via telefono dati personali, accertarsi sempre che il richiedente abbia titolo a richiederli e, in caso di dubbio o dati sensibili, ove possibile, utilizzare mezzi più sicuri di comunicazione;
- nel caso vengano comunicati dati personali e/o sensibili via fax, prelevare il fax senza lasciarlo in mostra in attesa di essere prelevato;
- prima di inviare ad un corrispondente via fax dati personali e/o sensibili accertarsi che sia personalmente pronto a riceverli e che non vengano abbandonati presso la macchina ricevente in attesa di essere prelevati;

LE CHIAVI DI ACCESSO AI DATI INFORMATICI, IN PARTICOLARE LE PASSWORD

Ogni utente del sistema viene identificato mediante una credenziale di autenticazione che lo identifica univocamente. Ad ogni utente riconosciuto vengono messi a disposizione i dati e gli strumenti che competono alla propria mansione. Possiamo quindi affermare che la combinazione di un nome utente (o user ID) e della password relativa costituiscono un codice di identità personale. Se consentiamo a qualcuno di operare con le nostre credenziali, sia che glie le abbiamo comunicate sia che lasciamo incustodito il terminale che abbiamo attivato mediante le nostre credenziali, questi verrà identificato dal Sistema come se fossimo noi.

Come detto, l'autenticazione dell'incaricato/utente avviene per mezzo della password. In merito, Vi sono diverse categorie di password, ognuna con una propria funzione precisa:

- Le chiavi di accesso (user ID e password) alla rete LAN aziendale permettono all'incaricato di essere riconosciuto come tale dal sistema di rete e, di conseguenza, di accedere alle risorse in esso contenute in base al proprio profilo d'utenza legato alla particolare chiave d'accesso. L'uso di tali chiavi di accesso, peraltro, impedisce che terzi non autorizzati possano accedere da una postazione alle risorse della rete.
- Le password di accesso dei programmi specifici (applicativi) permettono di restringere l'accesso ai dati processati da tali programmi al solo personale autorizzato.
- La password del salvaschermo, infine, impedisce l'accesso non autorizzato al proprio elaboratore (e alle risorse da questo accessibili) in caso di momentanea assenza dell'incaricato dalla propria postazione di lavoro.

Il salvaschermo. L'utilizzo di questo strumento di blocco del terminale e, quindi della possibilità che qualcuno acceda al sistema tramite un elaboratore lasciato incustodito, è senz'altro utile ma è bene fare attenzione ad un particolare: qualsiasi tempo di latenza venga impostato per l'attivazione del salvaschermo sarà sempre sufficiente a consentire l'accesso ad altri fra il momento in cui ci assentiamo dalla postazione a quello in cui il programma si avvia, che sia un minuto o dieci. L'ideale, quindi, è fare in modo che la funzione si possa attivare per mezzo di una combinazione di tasti o della selezione di una icona posizionata sul desktop o sulla barra di avvio veloce. I sistemi PC Windows collegati a dominio consentono il blocco del terminale mediante la pressione simultanea dei tasti CTRL + ALT + CANC (o DEL) seguiti dalla pressione del tasto INVIO (o ENTER). In questo modo il terminale si blocca immediatamente è potrà essere riattivato solo dall'utente che lo ha bloccato o da un amministratore di sistema.

È necessario che tutti gli incaricati imparino ad utilizzare questi tre tipi fondamentali di chiavi di accesso. Per quanto concerne la scelta delle password si rimanda alle indicazioni della sezione successiva.

È altresì necessario mantenere il massimo riserbo in relazione alle proprie chiavi di accesso ed è vietato comunicare ad altri incaricati la propria chiave di accesso (in tal caso, come già ricordato, terze persone accederebbero alle risorse di rete sotto l'identità digitale dell'incaricato e qualsiasi operazione abusiva venisse effettuata sarebbe attribuita alla responsabilità dell'incaricato identificato dalla chiave di accesso).

I files di office automation contenenti dati sensibili (stato di salute, vita sessuale, opinioni politiche, religiose, sindacali, origini razziali o etniche, dati provenienti dal casellario giudiziale) e/o giudiziari o altri dati di natura riservata devono essere salvati in rete nelle apposite directory ad accesso selezionato e, come detto, se salvati per necessità di lavoro su supporti magnetici od ottici (CD Rom, dischetti, cassette), devono essere protetti con password di accesso al documento o con sistemi di cifratura.
A questo scopo gli Amministratori di Sistema adottano, e trasmettono le modalità operative al personale, i sistemi di volta in volta valutati come maggiormente sicuri ed efficaci.

CUSTODIA DELLE PASSWORD

Le password devono essere mantenute segrete. Gli incaricati non devono scrivere la password in luoghi facilmente accessibili, né vicino alla postazione di lavoro. Se per esigenze di manutenzione dovesse essere necessario comunicare la propria password agli incaricati della manutenzione, al termine dei lavori di questi ultimi sarà necessario modificare la propria password.

In caso di assenza di un incaricato, il recupero di file, documenti o dati cui lo stesso incaricato aveva accesso esclusivo tramite le proprie credenziali di autenticazione, deve avvenire senza comunicazioni di password tra

colleghi. In tali casi, deve essere informato l'amministratore di sistema che, previa comunicazione all'incaricato assente, recupera i file, documenti o dati, rendendoli disponibili per le esigenze lavorative di terzi incaricati. Dopo tale attività all'incaricato può essere richiesto di modificare obbligatoriamente la password all'accesso successivo.

MODIFICA DELLE PASSWORD

Le password che completa la credenziale di autenticazione al dominio (user ID + password) può essere cambiata a discrezione dell'utente senza aspettare gli automatismi impostati dagli amministratori di sistema: quando sia stato necessario comunicarla a terzi (amministratori o incaricati), quando si abbia il sospetto che altri l'abbiano trovata o utilizzata. La possibilità di variare la password si ottiene mediante la pressione contemporanea dei tasti CTRL + ALT + CANC (o DEL) e la selezione dell'opzione "Cambio Password".

REGOLE INERENTI LE PASSWORD

Il più semplice metodo per l'accesso illecito a un sistema informatico consiste nell'indovinare la password dell'utente legittimo. In molti casi sono stati procurati seri danni al sistema informativo a causa di un accesso protetto da password "deboli". La scelta di password "forti" è quindi parte essenziale della sicurezza informatica.

Di seguito vengono riportate alcune regole, che rappresentano lo standard in materia. Sebbene riportino alcune ripetizioni rispetto a quanto già detto in precedenza, si è ritenuto opportuno segnalare nuovamente il principio al fine di sensibilizzare l'utenza dei servizi di rete.

COSA NON FARE

1. **NON** comunicare a nessuno la propria password: lo scopo principale per cui le password sono usate è assicurare che nessun altro possa utilizzare le risorse affidate all'incaricato o che terzi possano farlo a nome dell'incaricato stesso.
2. **NON** scrivere la password da nessuna parte che possa essere letta facilmente, soprattutto vicino al computer.
3. Quando si immettete la password nei form di richiesta, **evitare** che altri possano vedere i tasti che si battono sulla tastiera.
4. **NON** scegliere come password parole che si possano trovare in un dizionario delle principali lingue mondiali. Alcuni sistemi di forzatura delle password consistono in strumenti software che "provano" tutte le parole contenute nei dizionari per vedere quale sia quella giusta.
5. **NON** usare il proprio nome o altri dati anagrafici o di identificazione.
6. **NON** usare come password parole che possano in qualche modo essere legate alla propria persona come, ad esempio, dati del coniuge o familiari, ecc.

COSA FARE

1. **Cambiare la password** ogni qual volta richiesto dal sistema. Chiedere all'Amministratore di sistema quali sono le sue raccomandazioni sulla frequenza del cambio; a seconda del tipo di sistema l'intervallo raccomandato per il cambio può andare da tre a sei mesi.
2. Usare password lunghe almeno **8 caratteri** con un misto di lettere, numeri e segni di interpunzione., ovvero – laddove i sistemi gestiscano solo password di lunghezza inferiore – utilizzare password della lunghezza massima consentita dal sistema stesso.
3. Utilizzare password distinte per sistemi con diverso grado di sensibilità. In alcuni casi, le password viaggiano in chiaro sulla rete e possono essere quindi intercettate. Per cui, oltre a cambiarla spesso, è importante che sia diversa per quella usata da sistemi "sicuri". Il tipo di password in assoluto più sicura è quella associata a un supporto di identificazione come un dischetto o una carta a microprocessore; la password utilizzata su un sistema di questo tipo non deve essere usata in nessun altro sistema. In caso di dubbio, consultare l'Amministratore di sistema.
4. Qualora l'incaricato abbia notizia o timore che la propria password abbia perso la propria riservatezza deve modificarla immediatamente.

Come scegliere una password

Le migliori password sono quelle facili da ricordare ma, allo stesso tempo, difficili da indovinare, come quelle che si possono ottenere comprimendo frasi lunghe. La frase "Nel 2001 l'Inter ha perso il derby 6 a 0" può ad esempio fornire, tra le tante possibilità, "N2l'Ihpid6-0".
Ecco alcuni altri esempi:

Frase	Possibile password
Orzando si passa dal traverso alla bolina	OspdtaBo
Rosso di sera bel tempo si spera	RdSbTsSa
To be or not to be	(2B)V(2B)

TRACCIA DEI DATI RISERVATI

La cancellazione di un file da un supporto non comporta l'effettiva cancellazione delle informazioni in esso contenute: in altre parole, i dati non vengono effettivamente cancellati ma soltanto marcati come non utilizzati e sono facilmente recuperabili. Neanche la formattazione assicura l'eliminazione effettiva dei dati; solo l'utilizzo di un programma apposito (da richiedere all'Amministratore di sistema) garantisce che sul supporto non resti traccia dei dati precedenti. Nel dubbio, è sempre meglio usare un dischetto nuovo, distruggendo quelli già utilizzati e non più utili.

UTILIZZO DI ELABORATORI PORTATILI

I PC portatili sono un facile bersaglio per i furti. Se un incaricato ha necessità di gestire dati riservati su un portatile, è necessario salvare i documenti contenenti tali dati con password di protezione, ovvero, in caso di dati particolarmente riservati, è consigliabile l'utilizzo di un programma di cifratura del disco rigido. In tali circostanze sarà inoltre necessario procedere al salvataggio di backup dei dati in rete, al fine di garantire il loro recupero in caso di dimenticanza della password o di perdita del sistema di decriptazione.
Gli Amministratori di Sistema forniranno i sistemi di backup di volta in volta maggiormente idonei alla singola situazione.

DIVIETO DI UTILIZZO DEL COMPUTER DA PARTE DI PERSONALE ESTERNO

Salvo il caso di espressa autorizzazione da parte dell'Amministratore di Sistema, personale esterno non incaricato non deve accedere ad elaboratori aziendali. In caso di interventi di manutenzione (installazione di nuovo software/hardware nel computer), l'incaricato dovrà assicurarsi dell'identità della persona e delle autorizzazioni ad operare sul PC.

DIVIETO DI INSTALLAZIONE E UTILIZZAZIONE DI APPARECCHI NON AUTORIZZATI

L'installazione e l'utilizzo di apparecchi non autorizzati (in particolare apparecchi di comunicazione quali modem, schede telefoniche o dati, schede di rete e fax) su postazioni di lavoro collegati alla rete LAN aziendale offre una porta d'accesso dall'esterno non solo al computer, ma a tutta la rete aziendale senza protezioni.

Tale circostanza, espone a rischio di accesso abusivo tutti gli apparati e gli elaboratori connessi in rete e rende vani gli investimenti tecnologici effettuati dall'organizzazione per garantire la sicurezza di tutti gli asset del sistema informativo (firewall, sistemi di intrusion detection, ecc.).

È quindi vietata l'installazione da parte degli incaricati/utenti di apparecchi non autorizzati dall'Amministratore di sistema in elaboratori aziendali. Per l'installazione e/o l'utilizzo di apparecchi originariamente non implementati nell'elaboratore affidato all'incaricato/utente, quest'ultimo potrà farne richiesta al proprio Responsabile d'Area e al Responsabile dell'UO Sistemi informativi ed ottenere da questi specifica autorizzazione, sulla base delle vigenti procedure aziendali.

L'installazione dovrà essere curata dal personale tecnico autorizzato, in base alle vigenti procedure di sicurezza.

DIVIETO DI UTILIZZAZIONE DI PROGRAMMI NON AUTORIZZATI

L'elaboratore è consegnato all'incaricato con alcuni programmi preinstallati. Tali programmi permettono l'esecuzione delle operazioni di trattamento cui è preposto l'incaricato. Solo tali programmi e/o quelli successivamente installati dall'Amministratore di sistema, previa verifica della licenza d'uso, sono autorizzati.

Qualora per l'espletamento delle proprie mansioni sia necessario o utile l'utilizzo di programmi specifici, gli incaricati dovranno fare richiesta al proprio Responsabile d'Area ed ottenere da questi specifica autorizzazione, sulla base delle vigenti procedure aziendali.

L'installazione dovrà essere curata dal personale tecnico autorizzato, in base alle vigenti procedure di sicurezza. In ogni caso, è assolutamente vietata l'installazione di programmi sugli elaboratori da parte degli incaricati e ciò a prescindere dal tipo di licenza (shareware o freeware) che ne regolamenti l'utilizzo.

LINEE GUIDA PER LA PREVENZIONE DELLE INFEZIONI DA VIRUS

La prevenzione dalle infezioni da virus è molto più facile e comporta un impiego di tempo molto minore della correzione degli effetti di un virus; tra l'altro, permette di evitare conseguenze quali la perdita irreparabile di dati.

Un virus è un programma in grado di trasmettersi autonomamente e che può causare effetti dannosi. Alcuni virus si limitano a riprodursi senza ulteriori effetti, altri si limitano alla semplice visualizzazione di messaggi sul video, i più dannosi arrivano a distruggere tutto il contenuto del disco rigido.

COME SI TRASMETTONO I VIRUS DEGLI ELABORATORI

I virus si trasmettono:

- Attraverso programmi provenienti da fonti non ufficiali;
- Attraverso le macro dei programmi di automazione d'ufficio;
- Attraverso mail o risorse Internet.

QUANDO IL RISCHIO È ALTO

Il rischio di infezione da virus informatici è più elevato:

- Quando si installano programmi;
- Quando si copiano dati da dischetti o da memorie;
- Quando si scaricano dati o programmi da Internet.

EFFETTI DEI VIRUS

Gli effetti tipici dei virus posso essere rappresentati dal fatto che:

- Effetti sonori e messaggi sconosciuti appaiono sul video;
- Nei menù appaiono funzioni extra finora non disponibili;
- Lo spazio disco residuo si riduce inspiegabilmente;
- Alcuni documenti vengono cancellati o rinominati.

COME PREVENIRE I VIRUS

Di seguito vengono evidenziate alcune linee guida per la prevenzione da virus informatici.

UTILIZZARE SOLTANTO PROGRAMMI INSTALLATI DALL'AMMINISTRATORE DI SISTEMA

Copie non ufficiali di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato. È vietato l'uso di programmi non autorizzati, con particolare riferimento ai videogiochi, che sono spesso utilizzati per veicolare virus.

ASSICURARSI DI NON FAR PARTIRE ACCIDENTALMENTE IL VOSTRO COMPUTER DA DISCHETTO

In tali circostanze, se il dischetto fosse infettato, il virus si trasferirebbe nella memoria RAM e potrebbe espandersi ad altri files.

UTILIZZO DI SOFTWARE ANTIVIRUS AGGIORNATI

La tempestività nell'azione di bonifica è essenziale per limitare i danni che un virus può causare; inoltre è vitale che il programma antivirus conosca gli ultimi aggiornamenti sulle "impronte digitali" dei nuovi virus. Questi file di identificativi sono rilasciati, di solito, con maggiore frequenza rispetto alle nuove versioni dei motori di ricerca dei virus. Su tutti gli elaboratori deve essere quindi installato ed attivo un software antivirus. Tale software deve essere continuamente aggiornato. Questa regola rappresenta una misura minima di sicurezza imposta per legge. Il personale preposto alla gestione dei sistemi informativi provvede a curare un sistema di aggiornamento automatico degli antivirus installati sulle macchine assegnate agli incaricati/utenti e ad effettuare verifiche, almeno, semestrali in merito. Qualora un incaricato/utente si accorgesse del mancato funzionamento od aggiornamento del software

antivirus installato sul proprio elaboratore è pregato di darne immediata comunicazione personale preposto alla gestione dei sistemi informativi.