REGOLAMENTO INFORMATICO AZIENDALE

AZIENDA PER L'EDILIZIA ECONOMICA E POPOLARE DI CASTELFRANCO VENETO

Disciplinare interno ai sensi del Provvedimento Garante n. 13/07 del 1° marzo 2007

Approvato dal consiglio di amministrazione in data 13/06/2019

INDICE – REGOLAMENTO AZIENDALE PER L'UTILIZZO DI RISORSE INFORMATICHE, INTERNET E POSTA ELETTRONICA

REGOLAMENTO AZIENDALE PER L'UTILIZZO DI RISORSE INFORMATICHE, INTERNET E POSTA ELETTRONICA

1 SCOPO E AMBITO DI APPLICAZIONE

Scopo del presente documento è disciplinare l'utilizzo delle postazioni di lavoro da parte del personale dipendente della società AEEP (di seguito denominata Azienda). Le indicazioni contenute devono essere applicate per un corretto utilizzo delle risorse informative messe a loro disposizione per lo svolgimento delle proprie attività.

1.1 PRINCIPI GENERALI

Nell'impartire le seguenti prescrizioni l'Azienda tiene conto del diritto alla protezione dei dati personali, della necessità che il trattamento sia disciplinato assicurando un elevato livello di tutela delle persone, nonché dei principi di semplificazione, armonizzazione ed efficacia. Le prescrizioni potranno essere aggiornate alla luce dell'esperienza e dell'innovazione tecnologica. I trattamenti rispettano le garanzie in materia di protezione dei dati e si svolgono nell'osservanza dei principi di necessità, correttezza, per finalità determinate, esplicite e legittime osservando il principio di pertinenza e non eccedenza e nella misura meno invasiva possibile.
L'Azienda, utilizzando sistemi informativi per esigenze produttive o organizzative o, comunque, quando gli stessi si rivelano necessari per la sicurezza sul lavoro, si avvale legittimamente, nel rispetto dello Statuto dei lavoratori (art. 4, comma 2), di sistemi che potrebbero consentire indirettamente un controllo a distanza e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori. Il trattamento di dati che ne consegue è considerato lecito.
L'Azienda rispetta le procedure di informazione ai lavoratori in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati, nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori.

2 DESTINATARI

Destinatario del presente documento è da considerarsi tutto il personale dell'Azienda dotato di una stazione di lavoro informatizzata.

3 DESCRIZIONE DEL DOCUMENTO

Le risorse, hardware e software, in dotazione al personale aziendale quali personal computer, notebook, tablet, Smartphone, chiavette UMTS, stampanti, scanner, applicazioni gestionali e di business, software di base, strumenti di sviluppo, programmi di utilità, ecc. (d'ora in avanti "dispositivi informatici") costituiscono un valore strategico per l'Azienda e come tali devono essere adeguatamente protette.
Al fine di ridurre al minimo i rischi di indisponibilità, accesso non autorizzato, distruzione o perdita, anche accidentale, di informazioni l'Azienda ha definito:

- linee di comportamento atte ad impedire il presentarsi di problemi e/o minacce alla sicurezza nel trattamento dei dati
- regole per l'accesso, l'utilizzo e la protezione delle proprie risorse informative da parte del personale aziendale

L'utilizzo improprio della postazione di lavoro e/o l'introduzione di software diverso da quello fornito ed installato dal personale autorizzato dall' Azienda, potrebbe compromettere il corretto funzionamento dei

beni informatici e arrecare danni quali accessi abusivi, virus informatici, trattamento illecito, sia alle apparecchiature in dotazione che alla rete aziendale.

Gli utenti hanno diritto ad accedere alle risorse informatiche aziendali per le quali sono stati espressamente autorizzati e ad utilizzarle esclusivamente per gli scopi inerenti le mansioni svolte.

Pertanto, ogni soggetto è tenuto a:

- adottare, nell'ambito delle proprie attività, tutte le misure di sicurezza atte a prevenire la possibilità di accessi non autorizzati, furti, frodi, danneggiamenti, distruzioni o altri abusi nei confronti delle risorse informatiche
- attuare le suddette prescrizioni, anche attraverso l'adozione delle modalità d'utilizzo riportate nel presente documento, ed a segnalare eventuali violazioni alle medesime o situazioni che possano presentare dubbi relativamente alla sicurezza delle informazioni trattate.

4 LINEE GUIDA PER L'USO DEI DISPOSITIVI INFORMATICI

I dispositivi informatici (vedi par. 3) affidati al dipendente sono strumenti di lavoro ed ogni utilizzo non inerente l'attività lavorativa può generare disservizi e costi di manutenzione, pertanto gli utenti devono essere consapevoli delle loro specifiche responsabilità nella custodia e nel corretto utilizzo della propria stazione di lavoro. In particolare, si ricorda che ai sensi della vigente normativa in tema di tutela dei dati personali (Reg. UE 2016/679) gli incaricati ("autorizzati") del trattamento sono tenuti all'applicazione delle istruzioni impartite dal titolare.

4.1 CUSTODIA DELLA POSTAZIONE DI LAVORO

L'utente è direttamente responsabile dei dispositivi informatici a lui assegnati, pertanto:

- deve attivare manualmente lo screen saver in caso di assenza temporanea dall'ufficio attraverso la pressione simultanea dei tasti CTRL-ALT-CANC e la selezione dell'opzione "Blocca Computer", al fine di impedire durante l'assenza l'accesso alle applicazioni da parte di personale non autorizzato
- non deve modificare le caratteristiche impostate sul proprio PC. E' vietato installare software, sia esso freeware o di pubblico dominio, dispositivi quali modem e/o router esterni, chiavette per la navigazione Internet non previste nella configurazione standard del personal computer assegnato.

Oltre a quanto fin qui riportato, per i dispositivi mobili (notebook, smartphone, tablet, iPad ecc.) devono essere prese ulteriori misure cautelative al fine di custodirli con diligenza. È buona regola adottare ogni misura idonea a prevenire la sottrazione del dispositivo mobile o di parte di accessori del medesimo anche quando vengono lasciati all'interno dei locali lavorativi e non ed evitare di lasciare, anche solo temporaneamente, i dispositivi mobili incustoditi. In caso di furto o smarrimento di dispositivi informatici dotati di collegamento alla rete aziendale l'utente deve immediatamente avvisare il referente interno, individuato nella persona del sig. Massimo Melato, che attuerà i provvedimenti cautelativi del caso.

4.2 ACCESSO ALLE RISORSE INFORMATICHE

Gli strumenti adottati dall'Azienda per l'accesso alle risorse informatiche (es. codici di accesso, user-id, token crittografici) sono di uso strettamente personale e l'utente è tenuto a custodirli in modo appropriato.

Gli accessi alla rete aziendale, alla posta elettronica, al sistema di archiviazione della mail ed in generale a tutte le applicazioni aziendali sono regolati da uno o più set di credenziali individuali (composti da una

username ed una password), le quali dovranno essere custodite dal personale aziendale con la massima diligenza e non divulgate.

A fronte di problemi di accesso alle postazioni di lavoro riconducibili ad un errato inserimento della password, sia esso dovuto ad incuria nella digitazione o dimenticanza della stessa, che causano un blocco dell'account, si rimanda al paragrafo 5 ove viene specificata la corretta procedura da utilizzare dagli utenti per la richiesta di assistenza IT al personale autorizzato dall'azienda.

Il personale aziendale è tenuto a seguire le seguenti istruzioni:

- al termine di una sessione di lavoro sui server deve essere eseguito il blocco della sessione (CTRL-ALT-CANC + INVIO)
- non è possibile conservare sul proprio Personal Computer i dati inerenti alla propria attività lavorativa ma utilizzare le cartelle di rete messa a disposizione, siano esse ad accesso condiviso (share di gruppo) od esclusivo (share ad accesso riservato del singolo utente)
- non è possibile condividere sul proprio computer cartelle con altri utenti, in modo tale da evitare accessi non regolamentati e non controllati alla propria postazione
- non è consentito inserire una password di accensione (a livello di bios)
- non è consentito avere sulla propria postazione di lavoro e/o su share di rete materiale in formato elettronico di carattere personale (foto, documenti non attinenti alla mansione svolta, film, musica)
- non è consentito collegare alla rete aziendale (wired o wireless) qualunque tipo di dispositivo personale (notebook, smartphone, tablet, iPad, ecc.)
- non è consentito, salvo autorizzazione, il collegamento alla rete elettrica presente nella sede dispositivi elettrici quali phon, stufette, ebollitori, macchine da caffè, forni microonde, mini-frigo ecc. ecc.

4.3 UTILIZZO DEL SOFTWARE

Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dalle strutture preposte, così come non è consentito installare autonomamente programmi. Eventuali richieste di installazione devono essere inoltrate al referente interno, individuato nella persona del sig. Massimo Melato, che vaglierà la fattibilità e nel caso provvederà ad installare quanto richiesto (si rimanda al paragrafo 5 per un maggior dettaglio inerente le modalità di richiesta).

L' inosservanza di questa disposizione, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'Azienda a gravi responsabilità civili e penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (D. Lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore) che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.
A tal proposito l'Azienda effettua periodici controlli sui dispositivi informatici volti a rilevare l'eventuale presenza di software non autorizzato. Tale attività non prevede in nessun caso il monitoraggio, neppure preterintenzionale, delle attività del lavoratore o del contenuto di dati personali nel PC.

4.4 UTILIZZO DI DISPOSITIVI ESTERNI

NON è consentito l'utilizzo di qualsiasi dispositivo esterno **PERSONALE**.

Laddove si rendano necessari per fini lavorativi dispositivi quali chiavi USB, hard disk esterni, supporti ottici, schede di memoria SD/xD/CF… ecc. devono essere autorizzati, richiesti e acquistati secondo le procedure aziendali in essere.

4.5 PREVENZIONE DEI VIRUS INFORMATICI

Ogni personal computer affidato agli utenti è dotato di un software antivirus centralizzato ad aggiornamento automatico al fine di prevenire l'introduzione di virus informatici che possano compromettere l'integrità del software e delle stazioni di lavoro.

L'utente deve sempre tenere conto del fatto che il programma antivirus non fornisce una protezione assoluta ed in particolare tra due aggiornamenti consecutivi esiste una finestra temporale di rischio entro la quale si possono introdurre virus non ancora noti dal programma stesso.

Pertanto, sarà cura dell'utente rispettare le seguenti linee guida:

- Mantenere la configurazione del sistema operativo in modo da permettere la visualizzazione dell'estensione dei file. Tale accorgimento rende più difficile il mascheramento da parte di file potenzialmente pericolosi (programmi EXE e script di vario tipo) che impiegano estensioni doppie (es. "leggimi.txt.vbs" oppure logo.jpg.exe")
- È fatto divieto disabilitare o disattivare i servizi relativi al software dell'Anti-Virus
- Ripulire immediatamente le stazioni che si rivelino, o vengano segnalate, come infette, segnalando al referente interno, individuato nella persona del sig. Massimo Melato, qualsiasi sospetta presenza di virus che pregiudichi o abbia pregiudicato il sistema, ed eventualmente interrompendo qualsiasi attività nel caso in cui l'azione di ripulitura non andasse a buon fine. In tal caso è opportuno procedere alla disconnessione fisica dalla rete aziendale, scollegando il cavo di rete o spegnendo il dispositivo informatico.
- Porre la massima attenzione nel ricevere, per necessità di svolgimento della propria attività lavorativa, contenuti dalla rete Internet (es. documenti di testo, tabelle, ecc.) cercando di valutare l'attendibilità dal sito a cui si è collegati (ad es. valutando all'interno dell'URL la presenza di estensioni a dominio di dubbia liceità e/o utilizzo dell'indirizzo IP al posto del nome di dominio)
- Nell'utilizzo della posta elettronica:
  - ✓ evitare di aprire allegati che contengono un'estensione doppia o con estensione JS, VBS, SHS, PIF, EXE, COM o BAT ;
  - ✓ se si ricevono e-mail non richieste o con contenuti pubblicitari, evitare di seguire i collegamenti a indirizzi Web eventualmente presenti nel testo delle e-mail;
  - ✓ nel caso si riceva un messaggio di e-mail da una persona conosciuta, ma con un contenuto insolito, effettuare un controllo con il mittente prima di aprire l'eventuale allegato; infatti alcuni virus sono in grado di trasmettere messaggi con allegati che sembrano spediti da mittenti conosciuti;
  - ✓ evitare di cliccare su icone dall'apparenza innocua che ricordano applicazioni associate ad immagini o musica, mostrate dagli allegati di posta elettronica in quanto possono nascondere "worm".

4.6 CARTELLE DI RETE CONDIVISE

Le cartelle di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file personale o che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità.
All'interno di tali cartelle devono essere identificate dei folder, chiaramente riconducibili all'utente, che devono essere da lui utilizzate come repository del backup dei dati eventualmente conservati nella postazione di lavoro assegnata o come locazione per la conservazione dei documenti trattati nel proprio lavoro.

Particolare attenzione deve essere prestata alla duplicazione dei dati sulle unità di rete. È assolutamente da evitare un'archiviazione ridondante.

4.7 UTILIZZO DELLE STAMPANTI DI RETE

È cura dell'utente effettuare la stampa dei dati solo se questa è strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni in quanto è buona regola non dimenticare documenti nelle stampanti, fotocopiatrici o fax.

In caso di stampa di documento nelle stampanti poste in aree comuni il titolare della stampa dovrà:

- ✓ Recarsi immediatamente presso la postazione oggetto della richiesta di stampa
- ✓ Attendere il completamento dell'operazione di stampa e ritirare tutti i fogli generati
- ✓ Distruggere immediatamente i fogli stampati erroneamente
- ✓ Contattare immediatamente il referente interno, individuato nella persona del sig. Massimo Melato, segnalando eventuali blocchi o anomalie riscontrate in fase di stampa.

Analogamente per la trasmissione/ricezione via fax l'utente dovrà attendere il rapporto di trasmissione stampato dall'apparecchio fax.

4.8 UTILIZZO DI INTERNET

Il libero accesso alla rete Internet espone l'Azienda ed i Dipendenti a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge 22 aprile 1941 n. 633 sul diritto d'autore e normativa sulla privacy Reg. UE 2016/679, fra tutte), creando evidenti problemi alla sicurezza. Pertanto, si precisa quanto segue:

4.8.1 Principi generali

Il personal computer costituisce uno **strumento di lavoro** aziendale, necessario allo svolgimento della propria attività lavorativa. È quindi da ritenersi PROIBITA la navigazione in Internet attraverso il personal computer in dotazione per motivi diversi da quelli strettamente concernenti lo svolgimento dell'attività lavorativa stessa.
È inoltre fatto divieto all'utente, lo scarico e l'installazione di software prelevato da siti Internet o da altre fonti, così come ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
Inoltre, è vietata, salvo specifica ed esplicita autorizzazione della direzione aziendale:

- la partecipazione a forum non professionali
- l'utilizzo di chat (esclusi gli strumenti espressamente autorizzati)
- l'utilizzo di bacheche elettroniche
- le registrazioni in guest books anche utilizzando pseudonimi (o nicknames)
- l'utilizzo di social networks

4.8.2 Configurazione di sistemi e l'utilizzo di filtri che prevengano determinate operazioni

La navigazione Internet per gli utenti della rete aziendale è regolamentata in modo da tutelare l'azienda nell'ambito della vigente normativa attraverso un sistema di Web Filtering che consente la definizione e l'applicazione di policy sull'utilizzo di Internet.
Il sistema di Web Filtering offre una funzionalità di filtraggio Internet accurata in grado di bloccare spyware e altre minacce via web compresi virus, cavalli di Troia, worm, keylogging, phishing, etc.
Ai fini del controllo della regolarità del traffico internet e dell'efficienza della banda utilizzata, la navigazione Internet può essere sottoposta a monitoraggio e registrazione. In queste attività di monitoraggio e registrazione, a tutela ai dati personali, i nomi degli utenti sono anonimizzati automaticamente dal sistema; qualora ne sussistessero le condizioni legittime e solo con l'autenticazione

tramite opportune credenziali è possibile togliere l'anonimato per risalire all'utente che abbia compiuto una violazione. I log di navigazione vengono conservati per 30 giorni.

4.9 POSTA ELETTRONICA

La casella di posta elettronica assegnata all'utente è uno **strumento di lavoro** che rimane di esclusiva proprietà dell'Azienda, anche dopo la cessazione del rapporto lavorativo, pertanto le persone assegnatarie sono direttamente responsabili del corretto utilizzo e funzionamento, e devono mantenerla in ordine.
Si evidenziano le seguenti regole comportamentali:

- la posta elettronica non va utilizzata ai fini personali, ma unicamente a fini lavorativi e in questo senso il dipendente assegnatario della casella di posta elettronica ne autorizza sin da ora la consultazione da parte di soggetti espressamente autorizzati dal Responsabile aziendale, nell'ambito dei controlli da questa effettuati. La posta elettronica non va utilizzata come strumento di archiviazione dati, che viene assicurata attraverso altri canali, quali ad es. lo spazio messo a disposizione nelle unità di rete. In ogni caso il dipendente, salvo il caso fortuito o evento tecnico a lui non imputabile, si impegna a preservare il contenuto delle mail comprensivo di tutti i dati.
- la lista dei destinatari della corrispondenza elettronica deve essere strettamente limitata alle persone che hanno effettiva necessità di essere messe a conoscenza del contenuto del messaggio stesso:
  - ✓ il destinatario di una comunicazione A: (per competenza) è colui al quale deve giungere in quanto ci si aspetta che faccia e/o decida qualcosa
  - ✓ il destinatario di una comunicazione CC: (per conoscenza) è colui il quale deve essere semplicemente conoscere la comunicazione senza fare e/o decidere alcunché
- il comando "rispondi a tutti" deve essere utilizzato solo nel caso tutti i destinatari (compresi i destinatari "per conoscenza") abbiano effettiva necessità di essere informati della risposta
- la comunicazione di lavoro inquadrata all'interno di un'organizzazione deve rispondere a requisiti di efficienza e di pertinenza, ed in termini generali deve pertanto essere inviata solamente alla persona titolata a gestire l'informazione. Non effettuare pertanto escalation verso i responsabili della persona destinataria se non in caso di mancata risposta in tempi ragionevoli, meglio se indicati nel contenuto del messaggio originale
- è vietato l'utilizzo della posta aziendale per la partecipazione a dibattiti, forum o mailing-list salvo diversa ed esplicita autorizzazione o necessità legate alle attività lavorativa opportunamente giustificate
- sono da evitare messaggi estranei al rapporto di lavoro o alle relazioni tra colleghi;
- è obbligatorio controllare i file allegati ai messaggi di posta elettronica prima del loro utilizzo (non eseguire il download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

Nella configurazione standard, gli utenti aziendali assegnatari della casella di posta elettronica:

- accedono al server Exchange con credenziali a loro assegnate al momento della creazione dell'account.
- utilizzano un mailbox che può essere soggetta a parametri di configurazione specifici (arco temporale o dimensione massima) determinati dalla mansione dell'utente
- usufruiscono del servizio di backup centralizzato essendo i messaggi depositati direttamente sul server
- usufruiscono del servizio di archiviazione MailStore che tiene copia dei messaggi contenuti nella cassetta postale e archivia offline i più vecchi in base a parametri temporali.

4.9.1 Funzionalità di sistema che consentano di inviare automaticamente messaggi di risposta in modo automatico

È possibile abilitare la funzionalità di risposta automatica. In tale messaggio, ogni lavoratore, può indicare le informazioni per contattare un altro collega (ad esempio nome, e-mail e/o telefono) in caso di necessità o di urgenza.
In caso di assenza programmata e prolungata del lavoratore (superiore ai 3 giorni lavorativi), e nell'impossibilità di consultare la posta da remoto, il titolare della casella di posta elettronica deve provvedere ad impostare, mediante opportuna configurazione tramite Exchange, il messaggio di "fuori sede" nel quale specifica:

- la durata del periodo di assenza
- gli eventuali contatti e-mail alternativi

Nella comunicazione dell'assenza, propria o di colleghi di lavoro, è vietato specificare la motivazione dell'assenza, (es. per malattia, maternità ecc.) in quanto si tratterebbe di trattamento di dati sensibili non autorizzato dal titolare. L'Azienda mette a disposizione testi standard da utilizzare per tali necessità.

4.9.2 Utilizzo di file PST locali

Ad eccezione dei file PST già in uso alla data di approvazione del presente Regolamento informatico, è vietato l'utilizzo di file PST locali per il salvataggio dei messaggi di posta. Laddove ne verrà esplicitata richiesta, al fine di avere un più rapido accesso alle vecchie mail rispetto al sistema di archiviazione, in deroga verranno adottate le seguenti misure:

- creazione dei file PST su nas di rete, sottoposto a backup automatico centralizzato.
- configurazione attraverso regole di Outlook di un folder, distinta dal folder contenente i messaggi della casella di posta, collegata al PST salvato su nas di rete, dove l'utente potrà consultare i messaggi vecchi precedentemente archiviati.

4.9.3 Consultazione della posta elettronica privata

Per quanto concerne l'utilizzo di servizi di posta elettronica personali esterni all'azienda:

- Non sono consentiti quelli che implichino la configurazione di un client di posta basati su protocollo POP3 o IMAP
- È consentita fuori dall'orario di lavoro o durante la pausa pranzo l'accesso a servizi di posta elettronica tramite Webmail, se il sito specifico non è in contraddizione rispetto ai controlli che regolano la navigazione Internet.

4.9.4 Firma nelle mail aziendali

L'utente deve provvedere ad adeguare la propria firma nelle mail aziendali in modo uniforme allo standard aziendale. Non sono ammesse altre varianti di firma, salvo deroga autorizzata della Direzione aziendale o traduzione del testo stesso in altra lingua:

(nome e cognome)
(funzione)
XXXX Sr.l. - Via ……, n°……. (TV)
Tel. +39 ……- Fax +39 …….
www.XXX.it

I dati personali sono trattati in conformità a quanto previsto dal Reg. UE 2016/679 per finalità di carattere contrattuale, commerciale ed invio di informazioni. Le informazioni contenute in questo messaggio di posta elettronica e nei file allegati sono da considerarsi strettamente riservate. Precisiamo che eventuali vostre risposte e contenuti/allegati annessi al presente messaggio potranno essere visualizzati non direttamente dal destinatario ma dai soggetti fiduciari preposti che potranno agire per suo conto in caso di assenza.

4.9.5 Accesso alle mailbox aziendali

L'apertura di messaggi di posta, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, è subordinata all'intervento da parte di un altro soggetto (fiduciario) che verificherà il contenuto dei messaggi e inoltrerà al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa; l'Azienda provvederà alla redazione di apposito verbale informando il lavoratore interessato alla prima occasione utile. Il fiduciario potrà essere scelto dall'interessato liberamente tra i propri colleghi; in mancanza di individuazione, tale fiduciario coinciderà con il sig. Massimo Melato.

4.9.6 Gestione della mailbox aziendale in caso di cessazione del rapporto di lavoro

In caso di cessazione del rapporto di lavoro, l'Azienda provvederà all'inserimento di un avvertimento ai destinatari nel quale sia dichiarata la fine della collaborazione del dipendente con l'azienda. Il disclaimer sarà attivo per un periodo di tempo definito dalla Direzione aziendale in base alla mansione del lavoratore, e in ogni caso non superiore a 6 mesi. Durante tale periodo, al fine di gestire le nuove richieste, le e-mail in arrivo potranno essere inoltrate al fiduciario (vedi punto precedente). Trascorso il termine, la casella di posta elettronica del dipendente cessato verrà disabilitata.

4.10 TELELAVORO

Su richiesta, se giustificata da comprovati motivi che comportino l'assenza dal posto di lavoro, è possibile attivare la modalità di telelavoro mediante collegamento alla rete dell'azienda assicurato tramite VPN.
Il dispositivo/personal computer utilizzato per il collegamento VPN è da considerarsi dispositivo collegato alla rete aziendale, pertanto valgono tutti gli accorgimenti e prescrizioni per l'utente previste dal paragrafo 4 del presente paragrafo, sia durante la sessione di collegamento in VPN sia durante l'utilizzo del dispositivo/pc in locale.
È compito e responsabilità dell'utente assicurarsi che il sistema operativo del dispositivo utilizzato per il collegamento VPN sia aggiornato e che sia protetto da antivirus aggiornato.
Le credenziali fornite all'utente per il collegamento VPN sono personali e all'utente è proibito cederle o permettere ad altre persone il collegamento VPN alla rete aziendale.
Nell'attività di telelavoro è proibito trasferire/copiare file dalla rete aziendale al dispositivo locale sia in download che in upload.
A fini di controllo della regolarità dei collegamenti VPN alla rete aziendale e di efficienza nell'utilizzo della banda internet, l'orario di inizio, di fine e la durata dei collegamenti VPN di ogni utente potrà essere oggetto di monitoraggio e registrazione.
Per ottenere l'autorizzazione ad accedere all'infrastruttura informatica dell'Azienda mediante un collegamento diretto e sicuro (VPN), gli utenti VPN sono tenuti a prendere visione e ad accettare, sottoscrivendolo, il "Regolamento aziendale per l'accesso mediante VPN alle risorse informatiche", che è da considerarsi parte integrante del presente regolamento.
Eventuali deroghe al sistema di connessione remota sopra descritto possono essere autorizzate dalla Direzione aziendale previa valutazione delle singole richieste da parte degli utenti.

5 RICHIESTA DI ASSISTENZA

Per quanto concerne le richieste di assistenza IT siano esse relative a qualsiasi problematica inerente le postazioni di lavoro, ai dispositivi in genere (stampanti, scanner ecc.) e/o alle applicazioni aziendali e/o

generici dubbi su quale comportamento adottare, la procedura prevede l'inoltro di una mail al referente interno, individuato nella persona del sig. Massimo Melato, oppure l'apertura della richiesta a mezzo telefono.

Per richieste di assistenza relative a sblocco account o reset della password possono essere richieste solo dal titolare delle credenziali.

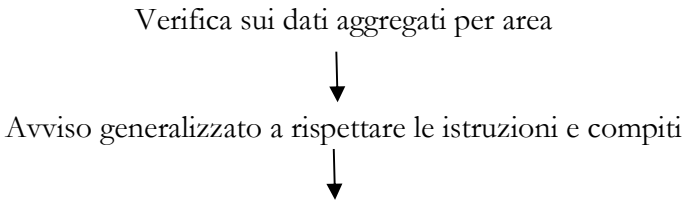
L'intervento risolutivo potrà essere eseguito direttamente sul PC dell'utente oppure attraverso collegamento remoto, il cui utilizzo è monitorato da apposito registro delle connessioni effettuate.

6 CONTROLLI

Controlli periodici e/o occasionali per ragioni legittime, specifiche e non generiche, verranno effettuati esclusivamente da soggetti autorizzati dalla Direzione aziendale.
Tali ragioni legittime possono essere:

- Verifica del corretto utilizzo degli strumenti di lavoro (es. pc aziendali);
- Evitare la perpetrazione di comportamenti illeciti e/o abusi informatici;
- Blocco del PC, infezione da virus non rilevato dal sistema di sicurezza;
- Guasto di elementi hardware che rendono impossibile la prosecuzione dall'attività lavorativa;
- Instabilità o blocco di sistemi software o della Linea Internet.

Graduazione dei controlli
I controlli iniziali, riferibili a navigazioni non aziendali e comunque non autorizzate, saranno riferiti alla totalità degli utenti. Il perdurare delle attività di navigazione non consentite autorizzano l'azienda a scendere ulteriormente nel particolare, effettuando controlli al livello di gruppi omogenei. In caso di estrema ratio, qualora si rilevino ulteriori abusi che possano precludere la sicurezza dei sistemi informativi, possano essere lesivi del patrimonio aziendale e possano identificare anche reati di natura penale, l'attività di controllo verrà effettuata con modalità di identificazione personale.



Modalità di controllo
I controlli verranno svolti nel rispetto della libertà e dignità dei lavoratori, nonché nel rispetto dei principi di correttezza, pertinenza e non eccedenza.

Coloro che dovessero violare quanto disposto dal presente regolamento aziendale saranno soggetti alle azioni disciplinari ai sensi dell'art.7 della Legge 300/1970.

7 SOGGETTI PREPOSTI

Nel caso di eventuali interventi per esigenze di manutenzione del sistema, sarà posta opportuna cura nella prevenzione di accessi illegittimi a dati personali presenti in cartelle o spazi di memoria.

I soggetti preposti al trattamento dei dati (in particolare, gli incaricati della manutenzione) svolgeranno solo operazioni strettamente necessarie al perseguimento delle relative finalità, senza realizzare attività di controllo a distanza, anche di propria iniziativa.
I soggetti che operano quali amministratori di sistema o figure analoghe cui siano rimesse operazioni connesse al regolare funzionamento dei sistemi sono edotti e consapevoli delle linee di condotta da tenere, attraverso un'adeguata attività formativa sui profili tecnico-gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto nelle comunicazioni.

8 ISTRUZIONI IMPARTITE DAL TITOLARE

Le presenti indicazioni operative sono rivolte a tutti gli incaricati del trattamento dei dati.

1) L'incaricato del trattamento dovrà aver accesso ai soli dati personali la cui conoscenza è strettamente necessaria per adempiere ai compiti a lui assegnati.
2) L'incaricato dovrà controllare e custodire gli atti e i documenti contenti i dati personali per l'intero ciclo necessario allo svolgimento delle operazioni.
3) All'incaricato compete la conservazione degli atti e dei documenti a lui affidati; l'incaricato stesso provvederà a restituirli al termine delle operazioni affidate.
4) L'incaricato, in caso di trattamento di dati sensibili o di dati giudiziari dovrà controllare e custodire gli atti e i documenti a lui affidati, fino alla restituzione, in maniera che ad essi non accedano persone prive di autorizzazione, e restituirli al termine delle operazioni affidate.
5) L'incaricato dovrà conservare e custodire i supporti non informatici contenenti la riproduzione di informazioni relative al trattamento dei dati sensibili o dati giudiziari osservando le misure sopradescritte.
6) L'incaricato, nelle operazioni di trattamento, dovrà ridurre al minimo i rischi di distruzione e perdita.
7) L'incaricato che effettua operazioni di trattamento mediante l'ausilio di strumenti elettronici o automatizzati dovrà utilizzare il codice identificativo e la parola chiave a lui forniti dal Titolare, attraverso l'Amministratore di Sistema, e custodirli con la dovuta riservatezza.
8) L'incaricato dovrà modificare la parola chiave al primo utilizzo e alle scadenze previste (ogni 6 mesi per il trattamento dei dati personali, ogni 3 mesi per il trattamento di dati sensibili e/o giudiziari) ricordando che la password dovrà essere composta da almeno 8 (otto) caratteri e non dovrà contenere riferimenti agevolmente riconducibili all'incaricato.
9) L'incaricato non dovrà lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento (seguendo le istruzioni operative impartite dall'Amministratore di Sistema o dagli incaricati alla manutenzione e gestione degli strumenti elettronici)
10) Nel caso di utilizzo di supporti di memorizzazione contenenti dati sensibili o dati giudiziari, l'incaricato potrà riutilizzarli qualora le informazioni precedentemente contenute non siano tecnicamente in alcun modo recuperabili, altrimenti dovranno essere distrutti.

8.1 NORME A CUI ATTENERSI PER EVITARE RISCHI PROVOCATI DAI VIRUS INFORMATICI

8.1.1 Fattori di incremento del rischio e comportamenti da evitare

I seguenti comportamenti, comportano un incremento dei livelli di rischio informatico:

- riutilizzo di supporti di archiviazione già adoperati in precedenza

- uso di software gratuito (o shareware) prelevato da siti internet o in allegato a riviste o libri;
- uso di chiavi USB non autorizzate;
- collegamento in rete, nel quale il client avvia solo applicazioni residenti nel proprio disco rigido;
- collegamento in rete, nel quale il client avvia anche applicazioni residenti sul disco rigido del server;
- uso di modem per la posta elettronica e prelievo di file da BBS o da servizi commerciali in linea o da banche dati;
- ricezione di applicazioni e dati dall'esterno, Amministrazioni, fornitori, ecc.
- utilizzo dello stesso computer da parte di più persone;
- collegamento in Internet con download di file eseguibili o documenti di testo da siti WEB o da siti FTP;
- collegamento in Internet e attivazione degli applets di Java o altri contenuti attivi;
- file allegati di posta elettronica.

8.1.2 Norme basilari di comportamento

PREMESSA: per supporti esterni di archiviazione si intendono tutti i dispositivi rimovibili il cui utilizzo in azienda è autorizzato dal Titolare del trattamento:
Floppy Disk; Cd-Dvd, sia registrabili che riscrivibili; Chiavi USB; Hard-Disk esterni; schede di memoria Flash (es. SD, CompactFlash, MemoryStick, ecc.)

Al fine di evitare problemi correlati ad infezioni informatiche, dovranno essere rispettate almeno le seguenti prescrizioni:

- i supporti esterni di archiviazione, sia quando vengono forniti sia quando vengono ricevuti, devono essere sottoposti a scansione da parte del programma antivirus;
- è obbligatorio sottoporre a controllo tutti i supporti esterni di archiviazione di provenienza incerta prima di eseguire o caricare uno qualsiasi dei files in esso contenuti;
- limitare la trasmissione di files eseguibili e di sistema tra computer in rete;
- non utilizzare i server di rete come stazioni di lavoro;
- non aggiungere mai dati o files ai supporti esterni di archiviazione contenenti programmi originali.

8.1.3 Regole Operative

- Tutti i computer della società devono essere dotati di programmi antivirus.
- Il Titolare deve assicurarsi che i computer delle società esterne, qualora interagiscano con proprio sistema informatico, siano dotati di adeguate misure di protezione antivirus.
- Il personale delle ditte addette alla manutenzione dei supporti informatici devono usare solo supporti esterni di archiviazione preventivamente controllati e certificati singolarmente ogni volta.
- Ogni PC deve essere costantemente sottoposto a controllo anti-virus.
- All'atto della individuazione di una infezione il virus deve essere immediatamente rimosso.
- Tutti gli utenti del sistema informatico devono sapere a chi rivolgersi per la disinfezione e l'informazione dell'infezione deve essere mantenuta riservata.
- Il personale deve essere a conoscenza che la diffusione dei virus è punita dall'art. 615 quinquies del Codice Penale.

- Il software acquisito deve essere sempre controllato contro i virus e verificato perché sia di uso sicuro prima che sia installato.

8.1.4 Caratteristiche di base del software antivirus

Il software antivirus deve essere sottoposto a costante e frequente aggiornamento (almeno due volte al mese) ed in particolare:

- gli aggiornamenti devono essere resi disponibili dal produttore, anche tramite Internet;
- deve essere particolarmente efficace contro i virus della nostra area geografica;
- deve poter effettuare automaticamente una scansione ogni volta che viene avviato un programma;
- deve poter effettuare una scansione automatica dei supporti esterni di archiviazione;
- deve accorgersi del tentativo di modificare le aree di sistema;
- deve essere in grado di effettuare scansioni a intervalli regolari e programmati;
- deve essere in grado di effettuare la scansione all'interno dei file compressi;
- deve mantenere il livello di protezione in tempo-reale;
- deve eseguire la scansione in tempo-reale;
- deve poter eseguire la rimozione del codice virale in automatico;
- in caso di impossibilità di rimozione i file non pulibili devono essere spostati una subdirectory predefinita;
- deve essere attivo nella protezione per Applet di ActiveX e Java contenenti codice malizioso;
- deve essere in grado di effettuare la rilevazione/pulizia dei virus da Macro sconosciuti;
- deve essere in condizione di rilevare e rimuovere i virus da macro senza file pattern con un grado di riconoscimento superiore al 97 %;
- deve essere in grado di riconoscere i codici virali anche in file compattati utilizzando qualsiasi programma di compressione e in qualsiasi ambiente operativo.
- Considerato che in sistemi basati su reti locali o su reti geografiche, aumenta il pericolo di diffusione dei virus, ove possibile il sistema antivirus deve essere centralizzato e predisposto a svolgere almeno le funzioni di:
  - ✓ distribuzione degli aggiornamenti sia dei motori di scansione che degli eventuali file "pattern";
  - ✓ controllo e monitoraggio degli eventi virali;
  - ✓ automatico spostamento in directory di "quarantena" di virus informatici risultati non pulibili;
  - ✓ avviso all'amministratore di sistema di rilevazione di virus e indicazione del file "infetto".