SERVIZIO SANITARIO REGIONALE BASILICATA

Azienda Sanitaria Locale di Potenza

Istruzioni Operative sulle corrette modalità di utilizzo degli strumenti per i dipendenti in Smart Working

Con il presente documento l'Azienda intende disciplinare le norme comportamentali che tutto il personale in servizio operante in Smart Working deve rispettare.

Per quanto non previsto in questo documento, si richiamano comunque nel loro complesso le norme di legge, compreso quanto previsto dal contratto collettivo nazionale di lavoro riguardanti i doveri dei lavoratori.

Le presenti Istruzioni hanno come scopo quello di indicare le misure organizzative aventi l'obiettivo di proteggere tutti i dati trattati dall'azienda.

Divieto di comunicazione e divulgazione

È fatto assoluto divieto di comunicazione e divulgazione di qualsivoglia dato che l'incaricato è autorizzato a trattare, se non previa autorizzazione del proprio responsabile del Servizio. Tale divieto si intende esteso anche al periodo successivo alla scadenza dell'incarico o del rapporto di lavoro.

ISTRUZIONI PER IL CORRETTO TRATTAMENTO DATI CON STRUMENTI ELETTRONICI

Utilizzo dei computer aziendali

Qualora gli strumenti di lavoro vengono messi a disposizione dall'azienda e sono quindi sotto la responsabilità dell'azienda stessa, si precisa che il dipendente affidatario del bene si impegna a:

a) Utilizzarlo solo per fini professionali e in relazione alle mansioni assegnate;
b) Custodirlo con cura evitando manomissioni, danneggiamenti o utilizzi, anche da parte di altre persone, per scopi non consentiti;
c) Rispettare le presenti istruzioni e le norme di buon comportamento;

Si precisa comunque che il dispositivo è e resta di proprietà dell'azienda, che ha facoltà di esercitare in qualsiasi momento ogni diritto previsto dalle disposizioni legislative vigenti.

I dipendenti e i collaboratori sono responsabili della corretta custodia del bene e:

a) Durante l'utilizzazione dello stesso dovranno comportarsi in maniera diligente e responsabile, garantendo l'integrità materiale e del suo impiego
b) In caso di danneggiamento, furto, smarrimento o utilizzo illecito, potranno essere attivate azioni di natura disciplinare e afferenti il risarcimento del danno come previsto dagli artt. 1218, 2043 e ss. cod. civ.

Ad ogni utilizzo del computer fisso o del portatile, l'addetto si assume la responsabilità del corretto utilizzo dello strumento nel rispetto delle istruzioni che seguono:

a) Le postazioni sono configurate secondo gli standard Aziendali e qualsiasi modifica deve essere autorizzata dall'Amministratore di sistema, responsabile dei servizi informativi;
b) E' vietata l'istallazione sul computer di qualsiasi tipo di software senza l'autorizzazione dei Sistemi Informativi Aziendali, al fine di prevenire l'istallazione di software pericolosi (quali ad esempio virus informatici che possono alterare la stabilità dei sistemi operativi) o sprovvisti di regolare licenza d'uso (d.lgs. 29 dicembre 1992, n. 518, L. 18 agosto 2000, n. 248);
c) In presenza di terzi, è necessario accertarsi che questi non possano leggere le informazioni sul PC;
d) E' fatto divieto di caricare sul PC dati estranei all'attività lavorativa;
e) Una volta attivato il PC, è opportuno non lasciare incustodita la postazione senza prima averne bloccato l'accesso;
f) L'utilizzo di eventuali supporti esterni - oltre a dover essere autorizzato – deve essere preceduto da una opportuna verifica che accerti:
    a. L'origine del supporto;
    b. Il suo contenuto;
    c. L'assenza di virus al suo interno.
g) Non è consentito utilizzare programmi informatici o strumenti per intercettare, falsificare, alterare o sopprimere per finalità illecite il contenuto di comunicazioni e/o documenti informatici.

L'azienda si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere potenzialmente pericolosi per la sicurezza del sistema, ovvero acquisiti o istallati in violazione di quanto previsto nel presente documento.

Utilizzo dei computer di proprietà del dipendente

Qualora il dipendente utilizzi propri device, gli strumenti devono essere dotati almeno delle seguenti misure minime

a) Software di base ed applicativo aggiornato
b) Antivirus installato ed aggiornato
c) Utilizzo dello spazio cloud aziendale per effettuare il backup dei dati

È obbligatorio l'uso corretto della propria password di accesso al PC, del cui utilizzo ogni incaricato è pienamente responsabile. È indispensabile che ciascun incaricato prenda nota delle buone modalità con cui è possibile selezionare parole chiave di difficile individuazione, seguendo le norme indicate di seguito. Qualora si abbia il sospetto che la propria password sia stata in qualche modo compromessa o venuta a conoscenza di terzi, si raccomanda di provvedere immediatamente alla sua sostituzione e riferire l'accaduto al responsabile aziendale. Ai fini di mantenere l'adeguata protezione della propria password:

a) la parola chiave prescelta non deve mai contenere riferimenti personali (nomi, date di nascita, ecc…), né dovrebbe rappresentare una parola in qualsiasi lingua o dialetto sufficientemente diffuso;
b) si suggerisce di selezionare una nomenclatura della password adeguatamente lunga (minimo 8 caratteri) e complessa (caratteri minuscoli, maiuscoli e almeno un carattere speciale);
c) si raccomanda di non utilizzare la stessa password utilizzata in altri sistemi di autenticazione, interni o esterni all'azienda, come ad esempio l'accesso al

proprio conto corrente bancario e/o altre attività non legate all'attività aziendale;

d) non è permesso condividere o concedere l'uso della parola chiave prescelta con alcun soggetto, interno o esterno all'azienda;
e) al momento in cui si sostituisce la propria password, la nuova selezionata dovrebbe essere diversa da quelle già utilizzate in precedenza.

Utilizzo di telefono mobile

In sede di eventuale consegna di un telefono cellulare, palmare, blackberry, smartphone, tablet o simili, il datore di lavoro ne disciplina l'uso per finalità diversa dall'esecuzione delle prestazioni lavorative.
Si precisa comunque che il dispositivo è e resta di proprietà dell'azienda, che ha facoltà di esercitare in qualsiasi momento ogni diritto previsto dalle disposizioni legislative vigenti.
I dipendenti e i collaboratori sono responsabili della corretta custodia del bene e durante l'utilizzazione dello stesso dovranno comportarsi in maniera diligente e responsabile, garantendo l'integrità materiale e del suo impiego.
In caso di danneggiamento, furto, smarrimento o utilizzo illecito, potranno essere attivate azioni di natura disciplinare e afferenti il risarcimento del danno come previsto dagli artt. 1218, 2043 e ss. cod. civ.
Si precisa inoltre che:

a) Il gestore telefonico fornisce i tabulati delle telefonate effettuate da ciascuna utenza dell'Azienda e che pertanto quest'ultima potrà, in caso di necessità, effettuare controlli sul corretto utilizzo;
b) I dati salvati sul telefono (rubrica, agenda) sono e restano di esclusiva responsabilità del singolo utente, che deve occuparsi di provvedere ai necessari back – up o salvataggi;
c) Qualsiasi problema, disfunzione o rottura del telefono, va comunicata al Servizio di apparenenza;
d) In caso di interruzione del rapporto di lavoro tutti i dati aziendali presenti nel telefono (es. rubrica telefonica) devono essere restituiti unitamente all'apparecchio.

Posta elettronica

La posta elettronica diretta all'esterno della rete informatica aziendale può essere intercettata da estranei, ed è pertanto sconsigliato l'invio di documenti di lavoro riservati senza l'utilizzo di adeguate protezioni.

L'invio di documenti o dati mediante posta elettronica deve sempre essere effettuato con le dovute cautele, quali accertarsi che il destinatario sia autorizzato a trattare i dati inviati, che l'indirizzo sia corretto, che il destinatario riceva correttamente i documenti inviati (ad es. mediante conferma di lettura), ecc.

L'invio dei documenti contenenti dati particolari o particolarmente sensibili con la posta elettronica va effettuato previa protezione del documento con una password. Quest'ultima dovrà essere condivisa con il destinatario prima dell'invio o comunque con un mezzo diverso dall'email, nel cui corpo NON dovrà essere segnata in chiaro la password prescelta.

In generale, nell'utilizzo della posta elettronica come strumento di lavoro e di comunicazione tra i dipendenti, e tra questi e i terzi, si raccomanda in particolare di rispettare i criteri minimi di utilizzo per cui NON è consentito:

a) Dar luogo o rispondere a email "tipo catena di Sant'Antonio" dall'indirizzo aziendale;
b) Inviare immagini, file, video o scherzi elettronici dall'indirizzo aziendale;
c) Aprire allegati non sicuri, o inviati da fonti sconosciute;
d) Cancellare, anche parzialmente, le e-mail aziendali inviate e/o ricevute, salvo diversa autorizzazione;
e) Cancellare, anche parzialmente, la rubrica aziendale;
f) Cliccare su link sconosciuti.

È invece obbligatorio eliminare tempestivamente messaggi "spam" o similari (onde evitare la diffusione di virus informatici).

Procedura d'emergenza

Qualora il Titolare necessiti di dover accedere al PC assegnato ad un dipendente ovvero alla Sua posta elettronica sarà onere del Responsabile del Servizio o della Direzione stabilirne le modalità che potranno essere diversificate area per area nel rispetto delle regole che seguono:

a) Il responsabile dell'area d'accordo con il dipendente potrà individuare i colleghi autorizzati ad accedere alla sua casella di posta elettronica e/o alla propria postazione di lavoro in caso di assenza programmata;
b) In caso di assenza non programmata, il dipendente potrà autorizzare anche telefonicamente il proprio responsabile o i propri colleghi ad accedere alla propria casella email e/o postazione di lavoro;
c) In casi di necessità/urgenza/impossibilità a contattare il dipendente assente, l'Amministratore di Sistema, su richiesta della Direzione, potrà provvedere a resettare la password dell'utente per consentirne l'accesso. Tale operazione verrà comunicata al dipendente non appena possibile. Al suo rientro, questi imposterà una nuova password;
d) In ogni caso, è fatto divieto di "rispondere" utilizzando l'account email del dipendente assente;
e) Ogni utente ha l'obbligo di inserire un messaggio automatico di assenza;
f) Qualora la parola chiave venga utilizzata in assenza dell'incaricato, a quest'ultimo non compete più alcuna ulteriore responsabilità, in merito a trattamenti non autorizzati o accessi non consentiti ai dati. La sua responsabilità verrà pienamente rimessa in essere non appena avrà avuto la possibilità di selezionare una nuova parola chiave e assumere quindi la piena responsabilità del corretto utilizzo.

ISTRUZIONI PER IL CORRETTO TRATTAMENTO DATI CON STRUMENTI CARTACEI

Consegna dei documenti via posta

Nel caso la consegna di documenti, originali o fotocopiati contenenti dati particolari o informazioni qualificate come riservate, avvenga per posta, si richiede l'utilizzo di tipi di spedizione che garantiscano di tracciare i movimenti del documento (ad es. raccomandata, etc.). Quale che sia il tipo di spedizione adottato, si raccomanda di accertare che esso consenta di avere prova certa del fatto che il destinatario abbia effettivamente ricevuto i documenti inviati e che essi siano giunti integri, e quindi non manomessi o alterati in fase di trasporto.

Custodia dei documenti all'esterno dei luoghi di lavoro

Qualora per motivi di lavoro vengano trasportati documenti all'esterno del luogo di lavoro, l'incaricato deve tenere sempre sotto controllo il plico, avendo cura altresì che nessun soggetto terzo non autorizzato possa vedere anche solo la copertina del documento in questione.

Conversazioni e comunicazioni telefoniche

Si raccomanda di non discutere, comunicare o comunque trattare dati aziendali se non si è certi che il corrispondente sia un incaricato autorizzato a trattare i dati in questione.

Si raccomanda la massima attenzione nella scelta dei luoghi ove svolgere le conversazioni telefoniche.

Social Network

La divulgazione di informazioni all'esterno dovrà avvenire nel rispetto del principio di segretezza e riservatezza, nel rispetto del proprio profilo di autorizzazione e sempre salvaguardando l'immagine aziendale dell'azienda.