ASLMediocampidano
Azienda socio-sanitaria locale

ALLEGATO 4 - POLA ASL MEDIO CAMPIDANO

LINEE GUIDA PER IL LAVORO AGILE

SALUTE E SICUREZZA DEI LAVORATORI

La presente informativa, conforme al D. Lgs 81/2018 e ss.mm.ii., contiene l'analisi dei rischi generali e dei rischi specifici connessi allo svolgimento del lavoro in regime di Lavoro Agile. L'obiettivo è quello di fornire adeguate indicazioni comportamentali alle quali il lavoratore dovrà attenersi per garantire la propria sicurezza e la salvaguardia della sua salute psicofisica.

1. **Individuazione dei luoghi di lavoro consentiti**

I luoghi consentiti per lo svolgimento dell'attività in lavoro agile possono essere:

- Il domicilio o altre sedi comunicate all'Azienda nell'ambito dell'Accordo individuale, Allegato A al POLA;
- Spazi aziendali in caso di emergenze (ad esempio in allerta rossa)

2. **Principi di prevenzione e protezione nello svolgimento delle attività in Lavoro agile**

Il lavoratore che svolge la propria mansione in regime di lavoro agile deve innanzitutto garantire che la propria postazione di lavoro abbia caratteristiche il più possibile equivalenti rispetto a quella fornita dall'azienda, secondo quanto previsto dalle normative vigenti in materia di salute e sicurezza sul lavoro.

3. **Ambienti indoor**

Il lavoratore, come previsto dalle Linee Guida della Direttiva n.3/17 della Presidenza del Consiglio dei Ministri, dovrà attenersi ai principi di salute e sicurezza nei luoghi di lavoro ed in particolare a:

→ norme di prevenzione incendi
→ requisiti igienici dei locali
→ istruzioni d'uso strumenti/dispositivi attrezzature/apparecchiature e comportamenti da tenere in caso di mal funzionamento
→ ergonomia, postazione VDT e uso dei dispositivi portatili, computer, tablet, ecc…
→ requisiti minimi di impianti di alimentazione elettrica e corretto utilizzo dell'impianto elettrico

È bene evitare di regolare la temperatura dentro l'abitazione a livelli troppo alti o troppo bassi (a seconda della stagione) rispetto alla temperatura esterna.
Nei locali nei quali si svolgono attività di vita o di lavoro deve essere garantito il ricambio dell'aria con mezzi naturali o artificiali in modo che le concentrazioni di sostanze inquinanti e di vapore acqueo, prodotti dalle persone e da eventuali processi di combustione, siano compatibili con il benessere e la salute delle persone.
Le attività lavorative non possono essere svolte in locali tecnici o locali non abitabili (ad es. soffitte, seminterrati, rustici, box).

4. Norme di Prevenzione incendi e gestione delle emergenze

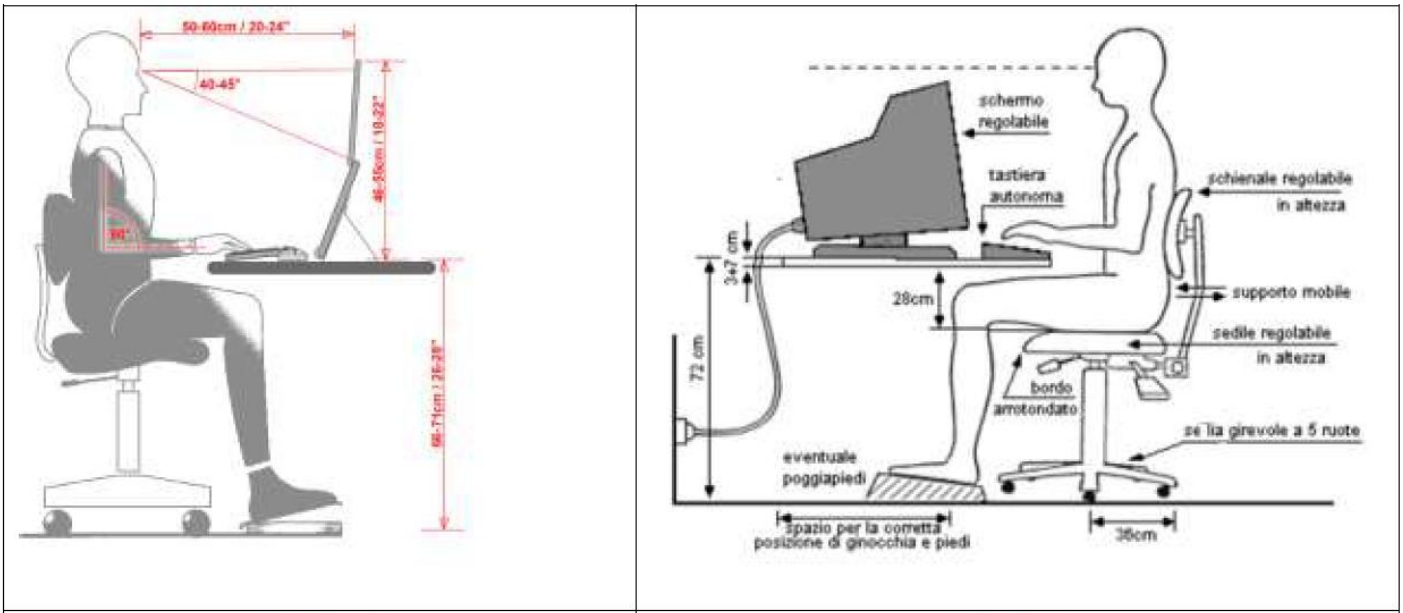
Comportamento per principio di incendio:
→ disattivare le utenze presenti (PC, termoconvettori, apparecchiature elettriche) staccandone il quadro elettrico generale dell'abitazione e/o stanza in cui si lavora;
→ avvertire i presenti all'interno dell'immobile o nelle zone circostanti, chiedere aiuto e, se necessario, chiamare i soccorsi telefonicamente (112.), fornendo loro le proprie generalità, luogo dell'evento, situazione ed affollamento, restando in attesa di eventuali indicazioni
→ solo se adeguatamente formati, provare a spegnere l'incendio attraverso i mezzi o metodologie di estinzione; (si ricorda di non utilizzare acqua per estinguere l'incendio su apparecchiature o parti di impianto elettrico);
→ se non si riesce ad estinguere l'incendio, abbandonare il luogo dell'evento (chiudendo le porte dietro di sé ma non a chiave) e aspettare all'esterno l'arrivo dei soccorsi per fornire indicazioni.

5. Efficienza ed integrità di strumenti/dispositivi e attrezzature/apparecchiature prima dell'uso
Prima di iniziare le attività, il lavoratore è tenuto a verificare che:

→ i cavi di alimentazione delle attrezzature elettriche siano adeguatamente protetti contro le azioni meccaniche (oggetti taglienti, ecc.) e termiche (caloriferi, ecc..);
→ l'attrezzatura di lavoro non presenti eventuali cavi danneggiati e con parti conduttrici a vista.
In caso contrario l'uso è vietato

6. Caratteristiche minime relative alla ergonomia della postazione dotata di VDT e nell'utilizzo di computer portatili, tablet, ecc.

La postazione ideale è quella rappresentata nelle figure seguenti:



Notebook	PC Fisso

Lo **schermo** deve essere facilmente orientabile ed inclinabile, posizionato frontalmente all'utilizzatore ad una distanza dagli occhi pari a 50-70 cm; il margine superiore deve essere posizionato leggermente più in basso rispetto all'orizzonte ottico dell'utilizzatore.

La **tastiera** deve essere separata dal monitor ed inclinabile rispetto al piano; deve essere posizionata frontalmente al video ad una distanza dal bordo della scrivania di almeno 10-15cm; deve possedere una superficie opaca, tasti facilmente leggibili e un bordo sottile e sagomato.

Il **mouse** deve essere posizionato sullo stesso piano della tastiera.

Il **piano di lavoro**

✓ deve avere una superficie poco riflettente;
✓ deve essere di dimensioni tali da permettere una disposizione regolabile dello schermo, dei documenti e del materiale accessorio,
✓ deve poter permettere di posizionare la tastiera ad almeno 15 cm di distanza dal bordo;
✓ deve possedere una profondità che assicuri un a corretta distanza visiva dallo schermo (almeno 50-70 cm);
✓ deve essere stabile e di altezza, fissa o regolabile, indicativamente fra 70 e 80 cm;
✓ deve avere uno spazio idoneo per il comodo alloggiamento e la movimentazione degli arti inferiori e per infilarvi il sedile.

È consigliabile, in caso di impiego prolungato di **computer portatili,** l'adozione di una tastiera, di un mouse o di un altro dispositivo, esterni, nonché di un idoneo supporto che consenta il corretto posizionamento dello schermo.

Il **sedile di lavoro** deve essere possibilmente girevole per facilitare cambi di posizione e stabile e permettere libertà nei movimenti. Deve possedere possibilmente la seduta possibilmente regolabile in altezza in maniera indipendente dallo schienale, lo schienale regolabile sia in altezza che in inclinazione, schienale e seduta con bordi smussati, rivestimento confortevole.

Se il basamento è dotato di ruote queste devono essere in numero non inferiore a cinque.
In ogni caso, anche se priva di ruote e/o con seduta non regolabile:

- la seduta deve essere comunque di altezza sufficiente per permettere l'alloggiamento e il movimento degli arti inferiori per cambiamenti di posizione nonché l'ingresso del sedile e dei braccioli (se presenti), sotto il piano di lavoro.
- Il sedile di lavoro deve essere stabile e permettere una posizione comoda; in caso di lavoro prolungato, la seduta deve avere bordi smussati.
- È importante stare seduti con un comodo appoggio della zona lombare.
- Durante il lavoro con il dispositivo mobile deve tenere la schiena poggiata al sedile provvisto di supporto per la zona lombare evitando di piegarla in avanti.
- Occorre mantenere gli avambracci, i polsi e le mani allineati durante l'uso di mouse e tastiera, evitando di piegare o angolare i polsi.
- Gli avambracci devono essere appoggiati sul piano e non sospesi.
- L'altezza del piano di lavoro deve essere tale da consentire all'operatore in posizione seduta di avere l'angolo braccio-avambraccio a circa 90°.
- In base alla statura, se necessario per mantenere un angolo di 90° tra gamba e coscia, creare un poggiapiedi con un oggetto di dimensioni opportune.

È importare evitare di esporsi a correnti d'aria fastidiose che colpiscano una zona circoscritta del corpo (ad es. la nuca, le gambe).

7. Corretto orientamento

Occorre posizionare il monitor in modo che le finestre non si trovino né di fronte, né di spalle e l'illuminazione artificiale sia al di fuori del campo visivo. Si eviteranno, in questo modo, fenomeni negativi quali abbagliamenti (finestra frontale) ovvero riflessi sullo schermo (finestra di spalle), causa principale di affaticamento visivo.

L'illuminazione artificiale dell'ambiente deve essere realizzata con lampade a tonalità calda provviste di schermi antiriflesso ed esenti da sfarfallio.
Le lampade devono essere collocate in modo tale da evitare abbagliamenti diretti e/o riflessi e la proiezione di ombre che ostacolino il campo visivo mentre si svolge l'attività lavorativa.
Occorre dotare le finestre del locale di idonei dispositivi di oscuramento che consentano, all'occorrenza, l'attenuazione della luce naturale e l'eliminazione degli eventuali riflessi presenti sullo schermo.

8. Indicazioni relative a requisiti e corretto utilizzo di impianti di alimentazione elettrica

Di seguito vengono riportate, a livello generale e non esaustivo, le principali indicazioni relative ai requisiti e al corretto utilizzo di impianti di alimentazione elettrica, apparecchi/dispositivi elettrici, dispositivi di connessione elettrica temporanea.

9. Impianto elettrico

Requisiti
→ l'impianto elettrico deve essere privo di parti danneggiate o fissate male;
→ le sue parti attive (es. conduttori di fase o di neutro) non devono essere accessibili (ad es. perché danneggiato l'isolamento);
→ i componenti dell'impianto elettrico non devono risultare particolarmente caldi durante il funzionamento;
→ le componenti dell'impianto ed i luoghi che li ospitano devono risultare asciutte/i, pulite e non devono prodursi scintille, odori di bruciato e/o fumo;
→ devono essere individuati, ove possibile, l'ubicazione del quadro elettrico nonché elementi/illustrazioni per riconoscere in generale gli interruttori in esso contenuti e le parti di impianto su cui operano.

Raccomandazioni nell'utilizzo
→ è buona norma che le zone antistanti i quadri elettrici, le prese e gli interruttori siano tenute sgombre e accessibili;
→ non devono essere accumulati o accostati materiali infiammabili a ridosso dei componenti dell'impianto per evitare innesco di incendi e/o deflagrazioni;
→ è importante posizionare le lampade, specialmente quelle da tavolo, in modo tale che siano mantenute lontane da materiali infiammabili;
→ non collegare tra loro componenti o accessori tra loro incompatibili
→ i principali mezzi di estinzione più adatti da utilizzare su parti elettriche in tensione sono gli estintori a CO2 e in subordine quelli a Polvere (ma rovinano le parti elettriche).

10. Apparecchi/dispositivi elettrici utilizzatori

Requisiti

→ gli apparecchi elettrici utilizzatori devono essere marcati CE;

→ gli apparecchi elettrici utilizzatori devono essere integri, non devono avere parti attive accessibili (es. conduttori di fase o di neutro dei cavi di alimentazione), non devono emettere scintille, fumo e/o odore di bruciato.

Indicazioni di corretto utilizzo

→ utilizzare apparecchi elettrici utilizzatori dotati di doppio isolamento;
→ accertarsi che durante l'utilizzo degli apparecchi elettrici non vengano occluse le griglie o le ventole di raffreddamento;
→ controllare che tutti gli apparecchi elettrici utilizzatori siano regolarmente spenti quando non utilizzati, specialmente se incustoditi per lunghi periodi;
→ gli apparecchi elettrici utilizzatori devono essere immediatamente disattivati tramite pulsante o interruttore di accensione in caso di guasto, dandone notizia al Datore di lavoro prima possibile;
→ inserire le spine dei cavi di alimentazione degli apparecchi elettrici utilizzatori in prese compatibili e farlo garantendo un contatto elettrico certo;
→ spegnere tutti i dispositivi e le attrezzature una volta terminato il lavoro o comunque quando non utilizzate.

11. Dispositivi di connessione elettrica temporanea (prolunghe, adattatori, prese multipla, avvolgicavo, ecc.)

In linea generale è bene collegare i cavi di alimentazione delle dotazioni informatiche direttamente alle prese dell'impianto elettrico senza riduttori, adattatori o prese multiple.

In assenza di un numero sufficiente di prese è necessario che i riduttori, gli adattatori o le prese multiple abbiano i seguenti requisiti

→ è fondamentale che i dispositivi di connessione elettrica temporanea siano marcati CE;
→ controllare che la potenza ammissibile dei dispositivi di connessione elettrica temporanea sia maggiore della somma delle potenze assorbite dai singoli apparecchi/dispositivi elettrici che devono essere alimentati;
→ i dispositivi di connessione elettrica temporanea che si intende utilizzare devono essere integri, non avere parti conduttrici scoperte (a spina inserita), non devono emettere scintille, fumo e/o odore di bruciato durante il funzionamento.

Indicazioni di corretto utilizzo

→ l'utilizzo di dispositivi di connessione elettrica temporanea deve essere ridotto al minimo indispensabile e preferibilmente solo quando non siano disponibili punti di alimentazioni più vicini e idonei;
→ a maggior ragione in questo caso, le spine dei dispositivi di connessione elettrica temporanea devono essere inserite in prese compatibili (spine a poli allineati in prese a poli allineati, spine schuko in prese schuko) e in modo tale da garantire un contatto elettrico certo;
→ è importante porre la dovuta attenzione a non piegare, schiacciare, tirare, tranciare cavi, prolunghe, spine, ecc.;
→ disporre i cavi di alimentazione e/o le eventuali prolunghe con attenzione, in modo da minimizzare il pericolo di inciampo;
→ fare attenzione a che i dispositivi di connessione elettrica temporanea non risultino particolarmente caldi durante il loro funzionamento; in tal caso verificare che la potenza ammissibile dei dispositivi di connessione elettrica temporanea sia maggiore della somma delle potenze assorbite dagli apparecchi/dispositivi elettrici che possono essere alimentati;
→ srotolare i cavi il più possibile o comunque disporli in modo tale da esporre la maggiore superficie libera per smaltire il calore prodotto durante il loro impiego.

12. Ambienti outdoor

Il lavoratore, come previsto alle linee guida citate nella direttiva n.3/17 della Presidenza del Consiglio dei Ministri, dovrà attenersi ai principi di salute e sicurezza nei luoghi di lavoro e in particolare a:
→ evitare l'esposizione diretta a radiazione solare e prolungata e a condizioni meteoclimatiche sfavorevoli;
→ evitare di lavorare in luoghi isolati o in cui sia difficoltoso richiedere e ricevere soccorso;
→ porre massima attenzione ai pericoli connessi alla presenza di animali, vegetazione in stato di degrado ambientale, presenza di rifiuti, ecc.;
→ evitare la presenza di sostanze combustibili o infiammabili e sorgenti di ignizione;
→ evitare di lavorare in luoghi in cui non ci sia la possibilità di approvvigionamento di acqua potabile.

13. Tempi di riposo e diritto alla disconnessione

Occorre rispettare i tempi di riposo di 15 minuti ogni 120 minuti di utilizzo del VDT.
È garantito il diritto alla disconnessione. Tale diritto di disconnessione si tramuta in obbligo di disconnessione nel periodo compreso tra le ore 22:00 e le ore 6:00 del giorno successivo (salvo eventuali casi legati a reperibilità, turnazione e lavoro notturno).

14. Conclusioni

Il lavoratore che svolge la propria prestazione lavorativa in regime di lavoro agile, per i periodi nei quali si trova al di fuori dei locali aziendali:
→ coopera con diligenza all'attuazione delle misure di prevenzione indicate dal datore di lavoro;
→ in caso venisse a mancare anche solo una delle condizioni di lavoro in sicurezza o in caso di anomalie o malfunzionamenti riscontrati nell'utilizzo delle attrezzature, è tenuto ad interrompere immediatamente la propria attività ed avvisare il proprio responsabile.

Il lavoratore garantisce che il proprio impianto elettrico è a norma di legge e che la postazione di lavoro rispecchia le caratteristiche minime di ergonomia sopra riportate.

Per ricevuta e accettazione

Data _____ Il Dipendente _____

NORME DI COMPORTAMENTO NELL'UTILIZZO DELLE DOTAZIONI INFORMATICHE PER I DIPENDENTI IN LAVORO AGILE

L'utilizzo di sistemi Informatici acceduti nell'espletamento della propria mansione da locazioni remote esterne al perimetro aziendale deve essere effettuato con la necessaria consapevolezza dei potenziali rischi sulla sicurezza dei sistemi aziendali prodotti dall'inosservanza di regole di comportamento messe in atto nell'attività in lavoro agile.
La Asl n 6 del Medio Campidano, con la presente, intende fornire idonee indicazioni e istruzioni al personale interessato. Le prescrizioni che seguono si aggiungono e integrano quanto previsto dal Regolamento U.E. 2016/679 e successive norme di armonizzazione e delle misure di sicurezza tecnica contenute nelle procedure aziendali in materia di utilizzazione delle dotazioni informatiche e della posta elettronica aziendale, per gli aspetti compatibili, con particolare riguardo all'uso della connessione VPN per l'attività in lavoro agile.

1. Rischi connessi ad un utilizzo improprio delle credenziali di accesso.

L'accesso ai sistemi informatici Aziendali tramite connessione remota VPN è consentita solo all'interno del territorio italiano. È consentito l'accesso da alcuni paesi dell'U.E. solo in via eccezionale e dietro specifica verifica e autorizzazione.

L'accesso ai sistemi informatici aziendali prevede l'utilizzo di credenziali (nome utente e password, ad personam), necessarie per accedere ai sistemi aziendali e come tali devono essere adeguatamente custodite.

In particolare per le password devono avere le seguenti caratteristiche:

→ devono essere costituite da almeno 8 caratteri;
→ devono contenere una varietà di caratteri il più possibile estesa (oltre ai caratteri dell'alfabeto, quelli numerici e quelli speciali ad esempio l!"f $%&/()=?" *+[ç@#0 §_-:.;,<>\]);
→ non devono essere banali, cioè reperibili in rete, non facilmente associabili alla persona, non essere ripetizione della *login* o una permutazione ciclica della stessa, né una stringa di caratteri contigui della tastiera.
→ devono sempre contenere caratteri maiuscoli e minuscoli;
→ devono essere cambiate con cadenza trimestrale, a meno di conseguente blocco dell'account, evitando il riutilizzo di chiavi già adottate nei 12 mesi precedenti;
→ al cambio password non possono essere utilizzate le ultime 4 impostate.

2. Rischi derivanti dall'utilizzo di dispositivi (personal computer, notebook, etc.) non adeguatamente aggiornati o non protetti.

È di fondamentale importanza che il dispositivo utilizzato nell'attività lavorativa in regime di lavoro agile sia mantenuto costantemente aggiornato, in particolare è necessario effettuare l'aggiornamento periodico del sistema operativo. È inoltre da evitare l'utilizzo di sistemi operativi obsoleti. L'accesso ai sistemi aziendali è consentito esclusivamente da computer dotati dei seguenti sistemi operativi:

→ Microsoft Windows Versione 7
→ Microsoft Windows Versione 8 e 8.1

→ Microsoft Windows Versione 10 o successive
→ Mac OS X o Linux (previa verifica tecnica della S.C. Sistemi Informativi Aziendali)
L'apparecchiatura utilizzata nell'attività lavorativa deve essere sempre dotata di un software antivirus costantemente aggiornato. A tal proposito, si segnala che le più recenti versioni dei sistemi operativi Microsoft mettono a disposizione o integrano strumenti antivirus quali Microsoft Security Essentials e Microsoft Windows Defender dei quali, comunque, si raccomanda di verificare periodicamente il loro regolare funzionamento e aggiornamento.

3. Rischi correlati all'utilizzo della casella di posta aziendale.

I messaggi presenti nella casella di posta elettronica aziendale possono contenere informazioni riservate o dati personali per i quali devono essere poste in essere tutte le attenzioni necessarie ad evitare un utilizzo fraudolento non autorizzato e, pertanto, l'accesso alla propria casella deve essere effettuato con le seguenti cautele:

→ la password utilizzata per l'accesso alla casella di posta deve soddisfare i requisiti minimi già precedentemente indicati;
→ se l'accesso viene effettuato attraverso l'uso delle funzioni *webmail* va sempre evitato il salvataggio delle credenziali di accesso. È importante, al termine della sessione di utilizzo della casella di posta, disconnettersi effettuando il c.d. "*logout*".

4. Rischi derivanti da comportamenti impropri.

Si raccomanda attenzione nella custodia di informazioni aziendali e dati personali utilizzati durante l'attività lavorativa, in particolare:

→ non memorizzare le proprie credenziali sui dispositivi utilizzati, soprattutto se utilizzati da più persone;
→ ridurre al minimo la possibilità che terze parti possano avere accesso alle informazioni, anche cartacee, trattate nell'ambito dell'attività lavorativa;
→ non assentarsi dalla propria postazione di lavoro senza avere chiuso la sessione del sistema operativo o bloccato lo schermo (CTRL+ALT+CANC e poi BLOCCA);
→ impostare la richiesta di credenziali di accesso al sistema operativo all'avvio del PC;
→ in caso di collegamento a terminal server RDP (Desktop Remoto) o connessione VPN, non utilizzare altro software presente sulla propria macchina, in particolare browser e client mail.
→ in caso di utilizzo di dispositivi portatili, non esporre questi ultimi a rischio di furto o smarrimento.

5. Riepilogo.

Requisiti minimi necessari per il collegamento telematico alla Rete della Asl n 6 del Medio Campidano:

→ Collegamento solo da dispositivi all'interno del territorio italiano (solo in via eccezionale e dietro specifica verifica e autorizzazione da alcuni ristretti Paesi dell'U.E.);
→ Personal computer dotato di sistema operativo Microsoft Windows 7, 8, 10 o successive con browser Microsoft EDGE o CHROME, ovvero Sistema Operativo Mac OS X o Linux previa verifica dei requisiti tecnici da parte della S.C. Sistemi Informativi Aziendali.
→ Collegamento a Internet attraverso linea di connessione dati ADSL o fibra con banda minima pari ad almeno 10 Mbps in downloa. In alternativa è consentito l'utilizzo di tecnologie di connessione dati basate

su rete cellulare, in tal caso i protocolli di collegamento dati dovranno garantire una velocità minima di connessione pari a 10 Mbps in download su tecnologie UMTS, HSDPA, LTE o 5G.
→ Al fine di ridurre il potenziale pericolo di attacchi informatici (virus worm, trojan, etc.) è obbligatorio:
• attivare sul proprio computer un software antivirus, avendo cura di mantenerlo costantemente aggiornato. Si ricorda che per i sistemi Microsoft è gratuitamente disponibile il sistema Antivirus Windows Defender.
• mantenere costantemente aggiornato il proprio Sistema Operativo installando le patch di sicurezza che periodicamente vengono distribuite dal produttore del Sistema Operativo.

Per ricevuta e accettazione

Data _____ Il Dipendente _____

PROTEZIONE DEI DATI PERSONALI IN LAVORO AGILE

Il presente documento contiene le istruzioni operative per i dipendenti della Asl n. 6 del Medio Campidano in materia di privacy e protezione dei dati personali, da utilizzarsi nell'ambito dello svolgimento della prestazione lavorativa in modalità di lavoro agile. Sono individuate nell'informativa le specifiche tecniche minime di custodia e sicurezza dei dispositivi elettronici e dei software, nonché le regole necessarie a garantire la protezione dei dati e delle informazioni.

Il "Lavoro Agile" impone la massima attenzione sui temi della riservatezza e presuppone che il dipendente rimanga sempre concentrato sulle modalità di lavoro, al fine di svolgere la propria attività (in parte all'interno dei locali aziendali e in parte all'esterno senza una postazione fissa) in modo corretto ed idoneo per proteggere l'operatività e la reputazione dell'Azienda.

A tal fine si richiamano i contenuti delle informazioni fornite ex artt. 13 e 14 Regolamento Unione Europea 679/2016 del 27 aprile 2016 e norme di armonizzazione per il trattamento dei dati personali e categorie di dati personali dei dipendenti, nonché della normativa interna dell'Ente in materia, con le obbligazioni ivi riportate a carico dei singoli dipendenti in relazione al ruolo ricoperto nel sistema privacy aziendale e in ottemperanza al principio della responsabilizzazione previsto dal sopraccitato Regolamento.

Per risorse informatiche, si intende qualsiasi risorsa (dati, informazioni, dispositivi quali pc, portatili, telefoni aziendali, sistemi, servizi etc…) messa a disposizione dall'Azienda e/o in possesso del dipendente necessaria a garantire l'attività lavorativa in modalità agile.

Il dipendente è responsabile del corretto uso delle risorse informatiche con particolare riferimento ai servizi, ai programmi cui ha accesso e ai dati trattati a fini istituzionali.

Al riguardo, si intende focalizzare l'attenzione sui seguenti accorgimenti per lavorare da remoto in modo sicuro:

1. Utilizzare le risorse rese disponibili messe dall'Azienda solo ed esclusivamente per lo svolgimento delle mansioni lavorative;

2. Non svolgere attività in lavoro agile al di fuori di ambienti privati protetti, che garantiscano la necessaria riservatezza della prestazione e/o connettendosi con collegamenti WIFI a reti aperte.
3. Accertarsi di usare sempre la VPN fornita dall' Azienda;
4. Per quanto riguarda il trattamento di dati personali mediante l'ausilio di strumenti elettronici, si richiamano le principali misure di sicurezza da adottare in caso di utilizzazione di strumenti di proprietà del dipendente e in particolare:

   → La password di accesso deve essere conservata con diligenza in modo che resti riservata, evitando sotto la responsabilità del dipendente, che altri ne vengano a conoscenza;

   → Il computer ed altri eventuali strumenti in dotazione e/o utilizzati per l'espletamento delle prestazioni di "Lavoro Agile" (P.C., smartphone, personali e/o aziendali ecc.), non devono essere lasciati incustoditi ed accessibili a persone non autorizzate. In caso di allontanamento anche temporaneo dalla postazione di lavoro il dipendente è tenuto a disconnettere la sessione di lavoro bloccando l'operatività del computer ("ctrl-alt-canc") e/o l'accesso allo smartphone (password di blocco schermo).

   → Non devono essere utilizzati dispositivi di memorizzazione esterna: come sopra riportato la documentazione inerente all'attività lavorativa dovrà risiedere esclusivamente sulle cartelle di rete, poiché tale modalità operativa è ritenuta adeguata a garantire che il trattamento è effettuato conformemente al Regolamento;
5. Configurare una password sul router Wi-Fi di casa che prevenga facili intercettazioni del traffico;
6. Tutti i computer, sia desktop che portatili, devono avere installato e attivo il software antivirus dell'Azienda o personale, con firewall attivato e devono essere mantenuti costantemente aggiornati con le patch di sicurezza del sistema operativo e degli applicativi utilizzati;
7. Usare sistemi operativi e software aggiornati all'ultima versione disponibile. Non installare software provenienti da fonti non ufficiali, in particolare programmi, software o file che violino la licenza d'uso, illegali o modificati illegalmente;
8. Non collegare dispositivi esterni (penna USB, Hard Disk esterni) di cui non si conosce la provenienza. Per salvare e o condividere le informazioni utilizzare sempre gli strumenti Aziendali che garantiscono maggior affidabilità oltre che il backup dei dati;
9. Prestare attenzione durante la navigazione in Internet evitando siti sconosciuti e rischiosi;
10. Durante la lettura della posta elettronica, evitare di scaricare allegati o cliccare su link ricevuti in e-mail da mittenti sconosciuti;
11. Utilizzare l'account di posta aziendale;
12. Effettuare sempre il log out dai Servizi/Portale Aziendali;
13. Usare sempre un atteggiamento misurato e attento per evitare di rivelare involontariamente informazioni riservate;
14. Le conversazioni tra il dipendente e gli altri interessati non devono essere oggetto di ascolto da parte di soggetti non autorizzati, i quali devono essere mantenuti ad una distanza che consenta di proteggere la confidenzialità; pertanto è obbligo del dipendente:

    → evitare di effettuare colloqui ad alta voce, di persona o per telefono, in presenza di soggetti non autorizzati a conoscere il contenuto della conversazione;

    → accertarsi che i conviventi o eventuali parenti e conoscenti non siano portati, anche involontariamente, a conoscenza di informazioni e processi attinenti l'attività lavorativa;

    → non utilizzare familiari o terzi per veicolare informazioni, anche se ritenute "banali", afferenti l'attività lavorativa;

→ nel caso di conversazioni telefoniche instaurate in seguito di chiamate inoltrate o ricevute, accertare, con cura, che l'interlocutore sia effettivamente un collega/utente/fornitore legittimato e autorizzato a conoscere le informazioni oggetto della comunicazione.

15. Il trattamento dei dati deve essere improntato ai principi di necessità, pertinenza e non eccedenza rispetto alle finalità degli stessi;
16. La protezione dei dati si applica anche a documenti cartacei, cui va garantita custodia e controllo. Pertanto, la documentazione cartacea contenente dati personali e amministrativa in genere, deve essere custodita per evitare l'accesso agli stessi da parte di soggetti non autorizzati.
17. Il dipendente deve prestare particolare attenzione quando si trasportano da un locale all'altro, da uno stabile all'altro, da un luogo ad un altro (mediante mezzi pubblici o privati o anche a piedi) documenti contenenti dati personali.
18. Più in dettaglio per quanto concerne l'utilizzo di documenti cartacei contenti dati personali e prelevati dagli archivi dell'Azienda, si sottolinea che il trasferimento di dati personali all'esterno della società deve essere giustificato da necessità strettamente correlate all'esercizio dell'attività lavorativa, agli obblighi di legge o alla difesa degli interessi della società. La circolazione dei dati personali cartacei, in situazione di mobilità deve essere ridotta al minimo indispensabile; i dati devono essere raccolti in porta documenti riportanti l'identificazione del dipendente utilizzatore e il suo recapito telefonico.
19. In particolare i documenti cartacei:

    → devono essere utilizzati solo per il tempo necessari allo svolgimento dei compiti assegnati e poi ripartiti negli archivi aziendali dedicati alla loro conservazione;

    → non devono essere lasciati incustoditi. Pertanto, nel caso di assenza, anche momentanea, dal luogo in cui si svolge "Lavoro Agile" è necessario chiudere a chiave i locali che ospitano i dati ovvero riporli dentro un armadio/cassetto chiuso a chiave; non devono restare, senza ragione, applicati su supporti che possono essere visionati da persone non autorizzate;

    → devono essere resi illeggibili prima di essere cestinati, qualora siano destinati a divenire rifiuti (ad es. strappando più volte la carta in modo che i contenuti diventino non decifrabili/non ricostruibili).
20. Per quanto riguarda la generica conservazione dei dati personali utilizzati dal dipendente in "Lavoro Agile" il Direttore/Responsabile della Struttura di appartenenza deve adottare soluzioni organizzative idonee a ridurre il più possibile i rischi di distruzione, perdita e accessi non consentiti ai dati anche in ambiente privato eletto dal dipendente.
21. L'Azienda, in qualità di Titolare, stabilisce che, ai sensi dell'art. 24 comma 1 del Regolamento U.E. 2016/679, la documentazione inerente all'attività lavorativa dovrà risiedere esclusivamente sulle cartelle di rete, poiché tale modalità operativa è ritenuta adeguata a garantire che il trattamento sia effettuato conformemente al Regolamento.
22. Se si ritiene di aver subito un incidente informatico (allarme antivirus che segnali un software pericoloso; apertura erronea di allegati di una mail insidiosa) deve essere comunicato l'accaduto con una mail ai sistemi informativi aziendali competenti (Dipartimento per la Sanità Digitale e l'Innovazione Tecnologica, Sistemi Informativi Amministrativi e Sicurezza ICT);
23. Il dipendente sarà specificatamente autorizzato al trattamento, informato e formato dal Datore di Lavoro (Titolare) in merito alle peculiarità del trattamento dei dati personali conseguenti alla modalità "Lavoro agile" della Sua prestazione lavorativa ed ai conseguenti rischi e misure di sicurezza adottate e da adottarsi, che integrano quelle fornite all'atto dell'autorizzazione ai trattamenti di competenza, in relazione al ruolo ricoperto nell'Ente.
24. I trattamenti dei dati effettuati dal dipendente devono rispettare il principio di necessità,

pertinenza e non eccedenza rispetto alle finalità degli stessi, avere scopi espliciti, determinati e leciti, come da istruzioni fornite in punto all'atto dell'autorizzazione al trattamento dati dell'Ente.

25. Nell'ambito delle proprie attività e in osservanza alle misure derivanti dal sistema procedurale, gestionale e tecnico instaurato dall'Azienda per garantire la sicurezza dei dati personali, il dipendente tratta dati:

    → esatti e, se necessario, aggiornati;

    → archiviati in una forma che consenta l'esercizio dei diritti da parte dell'interessato di cui al Capo III del Regolamento Europeo;

    → conservati in modo tale da consentire l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati;

    →ove necessario e compatibile, anonimizzati, pseudonimizzati o cifrati. Il dipendente dovrà, altresì, adottare le cautele previste per legge (diritto all'oscuramento e anonimato) nell'eventuale trattamento dei dati soggetti a maggior tutela ovvero dati particolarmente sensibili per i diritti e le libertà degli interessati (a titolo esemplificativo e non esaustivo: Legge n. 66/1996 Norme contro la violenza sessuale; Legge n. 269/1998 Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori quali nuove forme di riduzione in schiavitù; Legge n. 38/2006 Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet; Legge n. 135/1990 Programma di interventi urgenti per la prevenzione e la lotta contro l'AIDS; D.P.R. n. 309/1990 Testo unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza; Legge n. 194/1978 Norme per la tutela sociale della maternità e sull'interruzione volontaria della gravidanza; D.M. n. 349/2001 Regolamento recante: "Modificazioni al certificato di assistenza al parto, per la rilevazione dei dati di sanità pubblica e statistici di base relativi agli eventi di nascita, alla nati-mortalità ed ai nati affetti da malformazioni"; Legge n. 405/1975 Istituzione dei consultori familiari);

26. E' fondamentale sottolineare che è severamente sanzionata dal Regolamento (UE) 2016/679 la violazione dei dati personali, cioè la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
27. Tale violazione può afferire a una "violazione della riservatezza", in caso di divulgazione o accesso accidentale ai dati personali, alla "perdita della disponibilità" (comprese le ipotesi di sottrazione e/o furto), in caso di perdita o distruzione dei dati personali (accidentale o non autorizzata) e alla "violazione dell'integrità", in caso di alterazione non autorizzata o accidentale dei dati personali.
28. La violazione, in rapporto alla sua gravità, può comportare per l'Ente la Notifica del Data Breach, cioè la comunicazione della violazione dei dati personali all'Autorità di Controllo (Garante per la protezione dei dati personali), nonché, qualora ne abbiano un danno, ai soggetti i cui dati sono stati violati.
29. A tal fine si ribadisce l'obbligo del dipendente di segnalare qualunque ipotesi di violazione dei dati personali al responsabile della struttura preposto e al Responsabile della Protezione dei Dati, tempestivamente e, comunque, nei termini previsti dalla normativa interna aziendale in materia, anche al fine di consentire il rispetto dei ristretti termini di notifica all'Autorità di Controllo previsti dal Regolamento (UE) 2016/679, ove atto dovuto.
30. Prestare attenzione alla fuga di notizie ed in ogni caso avvertire il Titolare e il DPO per le notifiche

necessarie;

31. E' obbligazione contrattuale del dipendente rispettare dette istruzioni e partecipare alle attività formative previste dell'Ente in punto.
32. Il dipendente è consapevole ed accetta che la Asl Medio Campidano provvederà alla verifica del rispetto delle misure di sicurezza informatiche ed operative che indicate all'atto dell'autorizzazione alla modalità operativa del "Lavoro Agile", nel rispetto delle previsioni della normativa vigente in materia e dell'art.4 della L.300/70 e s.m.i..

Per ricevuta e accettazione

Data _____ Il Dipendente _____