P.O.L.A. - ALLEGATO_C

A TUTTI di DIPENDENTI
di AZIENDA CALABRIA LAVORO

Oggetto: **LAVORO AGILE - Smart Working**
Raccomandazioni di sicurezza nell'utilizzo di informazioni e strumenti tecnologici
Informativa sulla sicurezza dei lavoratori per il lavoro agile (L. n°81 del 22/052017)

Le presenti raccomandazioni vengono emanate dallo scrivente, nella qualità di datore di lavoro, come nozione comportamentale per i lavoratori di *Azienda Calabria Lavoro* che svolgono attività lavorativa in modalità *Smart Working* intese anche come informativa sulla sicurezza dei lavoratori ai sensi dell'art. 22, comma 1, della legge 22 maggio 2017 n. 81.

DISPOSIZIONI GENERALI - Obblighi e diritti previsti dalla L. 81/2017

- Il datore di lavoro garantisce la salute e la sicurezza del lavoratore, che svolge la prestazione in modalità di lavoro agile, e a tal fine consegna al lavoratore e al rappresentante dei lavoratori per la sicurezza, con cadenza almeno annuale, un'informativa scritta, nella quale sono individuati i rischi generali e i rischi specifici connessi alla particolare modalità di esecuzione del rapporto di lavoro.

- Il lavoratore è tenuto a cooperare all'attuazione delle misure di prevenzione predisposte dal datore di lavoro per fronteggiare i rischi connessi all'esecuzione della prestazione all'esterno dei locali aziendali.

- Ogni lavoratore deve prendersi cura della propria salute e sicurezza e di quella delle altre persone presenti sul luogo di lavoro, su cui ricadono gli effetti delle sue azioni o omissioni, conformemente alla sua formazione, alle istruzioni e ai mezzi forniti dal datore di lavoro.

- I lavoratori devono in particolare:

1. contribuire, insieme al datore di lavoro, ai dirigenti e ai preposti, all'adempimento degli obblighi previsti a tutela della salute e sicurezza sui luoghi di lavoro;

2. osservare le disposizioni e le istruzioni impartite dal datore di lavoro, dai dirigenti e dai preposti, ai fini della protezione collettiva ed individuale;

3. utilizzare correttamente le attrezzature di lavoro, le sostanze e i preparati pericolosi, i mezzi di trasporto, nonché i dispositivi di sicurezza;

4. utilizzare in modo appropriato i dispositivi di protezione messi a loro disposizione;

5. segnalare immediatamente al datore di lavoro, al dirigente o al preposto le deficienze dei mezzi e dei dispositivi di cui al punto 3 e 4, nonché qualsiasi eventuale condizione di pericolo di cui vengano a conoscenza, adoperandosi direttamente, in caso di urgenza, nell'ambito delle proprie competenze e possibilità e fatto salvo l'obbligo di cui al punto 6 per eliminare o ridurre le situazioni di pericolo grave e incombente, dandone notizia al rappresentante dei lavoratori per la sicurezza;

6. non rimuovere o modificare senza autorizzazione i dispositivi di sicurezza o di segnalazione o di controllo;

7. non compiere di propria iniziativa operazioni o manovre che non sono di loro competenza ovvero che possono compromettere la sicurezza propria o di altri lavoratori;

8. partecipare ai programmi di formazione e di addestramento organizzati dal datore di lavoro;

9. sottoporsi ai controlli sanitari previsti dal D. Lgs. 81/2008 o comunque disposti dal medico competente.

□ Il Datore di Lavoro ha provveduto ad attuare le misure generali di tutela di cui all'art. 15 del T.U. sulla sicurezza; ha provveduto alla redazione del Documento di Valutazione di tutti i rischi presenti nella realtà lavorativa, ai sensi degli artt. 17 e 28 D. Lgs. 81/2008; ha provveduto alla formazione e informazione di tutti i lavoratori, ex artt. 36 e 37 (attività in corso da dicembre 2019 e già programmata per l'anno 2020 con il S.P.P.) del medesimo D. Lgs. 81/2008.

COMPORTAMENTI DI PREVENZIONE GENERALE RICHIESTI ALLO SMART WORKER

Cooperare con diligenza all'attuazione delle misure di prevenzione e protezione predisposte dal datore di lavoro (DL) per fronteggiare i rischi connessi all'esecuzione della prestazione in ambienti indoor e outdoor diversi da quelli di lavoro abituali.

Non adottare condotte che possano generare rischi per la propria salute e sicurezza o per quella di terzi.

Individuare, secondo le esigenze connesse alla prestazione stessa o dalla necessità del lavoratore di conciliare le esigenze di vita con quelle lavorative e adottando principi di ragionevolezza, i luoghi di lavoro per l'esecuzione della prestazione lavorativa in smart working rispettando le indicazioni previste dalla presente informativa.

Evitare luoghi, ambienti, situazioni e circostanze da cui possa derivare un pericolo per la propria salute e sicurezza o per quella dei terzi.

Pertanto, di seguito, si procede all'analitica informazione, con specifico riferimento alle modalità di lavoro per lo smart worker al fine di mitigare e controllare i rischi di riservatezza, integrità e disponibilità delle informazioni di lavoro (con particolare riferimento ai segreti d'ufficio e ai dati personali) e degli strumenti tecnologici utilizzati presso il proprio domicilio - al di fuori dei locali dell'Ente - vengono dettate alcune raccomandazioni di sicurezza a cui sarà necessario attenersi per il corretto svolgimento del lavoro agile.

Le suindicate raccomandazioni vengono descritte nella Scheda n.3 in funzione di tre distinte fasi in cui organizzare giornalmente la propria postazione di lavoro agile:

Fase 1-Verifica della postazione di lavoro (Check in):

Fase 2 - Utilizzo della postazione di lavoro;

Fase 3- Riordino della postazione di lavoro (Check -out).

Si riportano in allegato le schede sintetiche sulle raccomandazioni e indicazioni che il lavoratore è tenuto ad osservare per prevenire i rischi per la salute e sicurezza legati allo svolgimento della prestazione in modalità di lavoro agile.

Il Responsabile Risorse Umane
Avv. Giovanni BONACCORSO

Il Commissario Straordinario
Dott. Felice IRACA'

Si allega:

SCHEDA 1 - Tutela della privacy da parte dei lavoratori in lavoro agile

SCHEDA 2 - Tabella Sintetica - Tutela della Privacy

SCHEDA 3 - Raccomandazioni di sicurezza per il corretto svolgimento del lavoro agile

AZIENDA CALABRIA LAVORO

ENTE PUBBLICO ECONOMICO STRUMENTALE DELLA REGIONE CALABRIA

Via Vittorio Veneto, n.60
89125 - Reggio Calabria (RC)
Pec: *postacertificata@pec.aziendacalabrialavoro.com*

SERVIZIO PREVENZIONE E PROTEZIONE

a.iacono@aziendacalabrialavoro.com

LAVORO AGILE - SMART WORKING

INDICAZIONI OPERATIVE PER L'ESECUZIONE DEL LAVORO AGILE, CON RIGUARDO ALLA SALUTE E ALLA PROTEZIONE DEI DATI PERSONALI

SCHEDE OPERATIVE

Raccomandazioni di sicurezza nell'utilizzo di informazioni e strumenti tecnologici
LAVORO AGILE INFORMATIVA SULLA SICUREZZA dei lavoratori
(art. 22, comma 1, della legge 22 maggio 2017 n. 81).

SCHEDA 1 - *TUTELA DELLA PRIVACY DA PARTE DEI LAVORATORI IN LAVORO AGILE*

SCHEDA 2 - *TABELLA SINTETICA - Tutela della Privacy*

SCHEDA 3 - *RACCOMANDAZIONI DI SICUREZZA PER IL CORRETTO SVOLGIMENTO DEL LAVORO AGILE*

SCHEDA 1

TUTELA DELLA PRIVACY DA PARTE DEI LAVORATORI IN LAVORO AGILE

Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio ("GDPR") D.lgs. n.196/2003 e ss.mm.ii. – *PRINCIPI COMPORTAMENTALI DIPENDENTI IN SMART WORKING.*

> I dipendenti devono svolgere i trattamenti previsti dalle rispettive mansioni nel rispetto delle prescrizioni e indicazioni operative contenute negli atti di individuazione quali persone autorizzate al trattamento, ai sensi dell'art. 29 del RGPD ("Regolamento Generale sulla Protezione dei Dati").

> Tali prescrizioni, aventi carattere "generico" anche allo scopo di adattarsi a situazioni emergenziali come quella in cui ci troviamo, sono perfettamente valide anche in un contesto di "lavoro agile". Nel rispetto delle circolari ministeriali in merito e la conseguente esigenza di regolamentare modalità lavorative che, di fatto, costituiscono una novità per questo ente, si ribadiscono alcuni concetti fondamentali e necessari al fine di effettuare un trattamento di dati personali conforme alla vigente normativa in un contesto di "lavoro agile", indipendentemente dalle diverse modalità di applicazione.

> Ad integrazione delle norme comportamentali richieste per tutti gli incaricati al trattamento in materia di protezione dei dati personali si forniscono le seguenti informazioni finalizzate ad assicurare che la prestazione lavorativa da svolgere in forma agile venga espletata nel rispetto dei principi di liceità, correttezza, riservatezza e moralità.

> L'attività svolta in modalità smart working deve rispettare le medesime disposizioni e normative in materia di protezione dei dati personali già previste nell'ambito dell'attività svolta presso la sede di lavoro. Il dipendente che accede al lavoro in modalità smart working deve essere consapevole che lo svolgimento di un'attività al di fuori della sede preposta comporta una maggiore attenzione nel preservare la confidenzialità e la riservatezza delle informazioni in suo possesso a cui potenzialmente possono avere accesso terzi non autorizzati.

> Si ribadisce che, a norma di legge e di contratto, i dipendenti sono tenuti alla più assoluta riservatezza dei dati e delle informazioni in loro possesso e/o disponibili sui sistemi informativi regionali, e che, conseguentemente, gli stessi dovranno adottare, in relazione alla particolare modalità della loro prestazione, ogni provvedimento e misura idonei a garantire tale riservatezza.

> Inoltre, nella qualità di "Incaricati del trattamento dei dati personali", anche presso il loro luogo di svolgimento della prestazione lavorativa fuori dalla sede ordinaria di lavoro, dovranno osservare tutte le misure di sicurezza previste nella relativa lettera di nomina di cui è già stata presa visione.

> In considerazione della autorizzazione VPN con riferimento alla modalità smart working, il dipendente ha accesso fuori dall' usuale ambiente di lavoro a molteplici dati di proprietà regionale e, pertanto, si richiama ancor più l'attenzione sui seguenti punti:

- porre ogni cura per evitare che ai dati possano accedere persone non autorizzate presenti nel luogo di svolgimento della prestazione lavorativa fuori dalla sede ordinaria di lavoro proteggendo il dispositivo attraverso password da non trasferire a terzi;

- procedere a bloccare il dispositivo informatico/persona! computer utilizzato in caso di allontanamento dalla postazione di lavoro, anche per un intervallo molto limitato di tempo;
- al termine della prestazione lavorativa giornaliera ed in ogni pausa di lavoro, è necessario conservare e custodire documenti eventualmente stampati e tutta la documentazione relativa all'attività di lavoro;
- qualora occorra trattenere presso il luogo di svolgimento della prestazione in smart working documentazione cartacea contenente dati personali, quest'ultima al termine del lavoro, dovrà essere conservata in armadi, cassetti o altri contenitori muniti di serratura;
- utilizzare i sistemi ed i programmi informatici messi a disposizione dall'amministrazione regionale nell'esclusivo interesse d'ufficio, non consentendo assolutamente ad altri l'utilizzo degli stessi.
- i sistemi informatici adoperati devono essere protetti attraverso password di sistema da non trasferire a terzi. Si consiglia un rinnovo della password con cadenza settimanale.

S C H E D A 2

Tabella Sintetica - TUTELA DELLA PRIVACY

TUTELA DELLA PRIVACY
SINTESI DEI PRINCIPI COMPORTAMENTALI DIPENDENTI IN SMART WORKING.

> Non salvare documenti di ufficio sul PC personale, se non temporaneamente e poi cancellarli immediatamente (specie se contengono informazioni personali);

> Porre attenzione nell'inviare foto per far vedere che si è in lavoro agile con sul monitor dati personali;

> L'accesso a dati aziendali non è più rischioso in lavoro agile, la pericolosità dipende da come lo strumento e l'operatore gestiscono il dato, non dalla locazione della persona;

> È buona norma avere sistema operativo e antivirus aggiornati; proteggere l'accesso ai dispositivi informatici (computer, tablet, smartphone) e delle connessioni (cablate o Wi-FI) attraverso l'uso di password sicure: si consiglia di utilizzare password lunghe e prive di riferimenti ai dati anagrafici;

> Creare un account specifico per l'uso nei momenti di lavoro, se il pc è usato anche da familiari o conviventi:

> In caso ci si allontani dal pc, bloccare il pc in modo che non sia utilizzabile da altri;

> Non incollare post-it sul pc personale le password per accedere agli applicativi di lavoro;

> implementare sistemi di backup per assicurare la disponibilità di dati e informazioni

> Passando a modalità di "lavoro agile" più avanzate, nel caso in cui sia possibile per i lavoratori effettuare l'accesso alla rete interna dell'ente dall'esterno, ciò va fatto necessariamente tramite una VPN, vale a dire un collegamento privato crittografato e, quindi, sicuro.

> Vanno evitate modalità che garantiscono standard di sicurezza molto inferiori come l'apertura di porte. Una soluzione che unisce le potenzialità di condivisione di dati e informazioni in tempo reale (così come avviene in un sistema server-client come quelli che caratterizzano la rete interna di Azienda Calabria Lavoro - su piattaforma Siar regionale) e le possibilità di coordinamento, gestione e rendicontazione del lavoro svolto da remoto è quella di servirsi di servizi cloud messi a disposizione dall'Amministrazione (es. Zimbra);

> Sono sconsigliati servizi cloud come quelli messi a disposizione a titolo gratuito da provider privati;

Si segnala che il Garante per la protezione dei dati personali ha raccomandato ai titolari del trattamento, quali le pubbliche amministrazioni, di astenersi dall'effettuare iniziative autonome di raccolta sistematica e generalizzata di dati riguardanti lo stato di salute dei lavoratori che non siano normativamente previste o disposte dagli organi competenti.

Resta comunque fermo l'obbligo del lavoratore di segnalare al datore di lavoro qualsiasi situazione di pericolo per la salute e la sicurezza sul luogo di lavoro. A riguardo, il Ministro per la Pubblica Amministrazione ha fornito indicazioni operative sull'obbligo per il dipendente pubblico di segnalare all'amministrazione la provenienza da un'area a rischio.

Affrontando alcuni aspetti che riguardano la salute qualche riflessione meritano, non tanto quelli legati all'affaticamento visivo (i moderni schermi LCD hanno limitato enormemente le criticità dei vecchi monitor a tubo catodico) quanto piuttosto quelli legati alla postura, è necessario infatti concedersi frequenti esercizi per "sgranchirsi" durante l'esecuzione del lavoro seduti davanti al computer.

Si ricorda che il limite di uso del computer è di 20 h settimanali e di interrompere per 15 minuti dopo 120 minuti al videoterminale.

SCHEDA 3

RACCOMANDAZIONI DI SICUREZZA PER IL CORRETTO SVOLGIMENTO DEL LAVORO AGILE

Di seguito, si procede all'analitica informazione, con specifico riferimento alle modalità di lavoro per lo *smart worker* al fine di mitigare e controllare i rischi di riservatezza, integrità e disponibilità delle informazioni di lavoro (con particolare riferimento ai segreti d'ufficio e ai dati personali) e degli strumenti tecnologici utilizzati press il proprio domicilio - al di fuori dei locali dell'Ente - vengono dettate alcune raccomandazioni di sicurezza a cui sarà necessario attenersi per il corretto svolgimento del lavoro agile.

ORGANIZZAZIONE GIORNALIERA DELLA PROPRIA POSTAZIONE DI LAVORO AGILE:

Fase 1-Verifica della postazione di lavoro (Check in):
Fase 2 - Utilizzo della postazione di lavoro;
Fase 3- Riordino della postazione di lavoro (Check -out).

FASE 1 - VERIFICA DELLA POSTAZIONE DI LAVORO (Check-in)

Nel caso in cui il proprio PC (personal computer) sia condiviso con familiari e/o coniventi, assicurarsi di disporre di un account specifico di lavoro, creato esclusivamente per lo svolgimento della prestazione lavorativa in modalità agile.

Verificare che il sistema operativo del proprio PC sia aggiornato all'ultima versione disponibile.

Verificare che sul proprio PC sia installato e attivo un antivirus aggiornato all'ultima versione disponibile.

Verificare che sul proprio PC siano state installate applicazioni provenienti da fonti non attendibili. In caso contrario, procedere rapidamente alla loro rimozione.

Verificare la robustezza delle diverse password utilizzate per accedere al proprio PC e alle applicazioni informatiche dell'Ente: nel dettaglio la propria password è considerata robusta se:

- ha una lunghezza di almeno 8 caratteri;
- è formata da una combinazione di lettere maiuscole, lettere minuscole, numeri e caratteri speciali (ad es. simboli di punteggiatura);
- viene cambiata periodicamente (si raccomanda il cambio settimanale).

Nel caso in cui occorre trattenere documentazione cartacea (ad es. stampe di documenti realizzate direttamente presso il proprio domicilio o altri documenti di lavoro in generale), assicurarsi di disporre di un armadietto, cassetto o altro contenitore munito di serratura, per la loro custodia.

FASE 2 - UTILIZZO DELLA POSTAZIONE DI LAVORO

Custodire con cura le password di accesso al proprio PC ed alle applicazioni informatiche dell'Ente:
- evitare di comunicarli a terzi;
- evitare d trascriverle su file memorizzato sul proprio PC;
- evitare di trascriverle su post-it o fogli lasciati in prossimità della postazione di lavoro;
- evitare di riutilizzarle per registrazioni personali a siti web e servizi Internet.

Nel caso in cui ci si allontani dal proprio PC, anche per un intervallo di tempo molto limitato, assicurarsi di bloccare l'accesso al proprio account.

Limitare in generale il tempo di permanenza sul proprio PC, di qualsiasi documento/file di lavoro, al tempo strettamente necessario alle relative attività di lavorazione / consultazione. Non appena saranno completate tali attività, qualora sia necessario salvare alcuni documenti / file, procedere con l'upload degli stessi verso le opportune applicazioni informatiche e/o specifici file repnsitory eventualmente predisposti dall'Ente (si consiglia di adoperare la funzioone "valigetta" dal proprio account Zimbra). Procedere quindi, dopo tale periodo di lavorazione, con la completa cancellazione dal PC di tutti i documenti / file trattati nell'ambito dell'attività svolta. Nell'applicare la presente raccomandazione, gestire con priorità casi in cui i documenti / file contengano anche dati personali e/ o segreti d'ufficio.

Evitare di salvare documenti/file di lavoro:
- su dispositivi personali di archiviazione di massa, rimovibili ad esempio: Unità a Stato Solido (SSD) e Hard Disk (HDD) esterni, Pendrive, DVD, CD (preferire quelli dotati di un sistema di crittografia hardware dei dari in essi contenuti). Nel caso in cui si rendesse necessario utilizzarli si raccomanda di custodirli con particolare attenzione e cancellarne il contenuto al termine dell'operazione che ne ha reso indispensabile l'utilizzo;
- su media di archiviazione e condivisione online privati, ad esempio: Google Drive, Dropbox. OneDrive, Box, iCloud Drive, ecc.

Prima di dar seguito ad ogni richiesta di informazione, pervenuta via mail, telefono o altro canale di comunicazione, verificare sempre l'identità dell'interlocutore al fine di evitare attacchi di "social engineering". Sospettare sempre, in particolare, di eventuali telefonate o mail esterne all''Ente in cui si chiedono password, informazioni su persone o aspetti strettamente riservati circa la propria attività lavorativa.

Allorquando siano presenti persone, in prossimità della propria postazione di lavoro agile, che possono acquisire, volontariamente o involontariamente, informazioni di lavoro, si raccomanda di gestire con particolare attenzione, ed eventualmente sospendere fino al loro allontanamento, tutte le attività lavorative che trattano dati personali e/ o informazioni strettamente riservate.

Si raccomanda in particolare di prestare attenzione a:
- conversazioni a voce alta al telefono o in conferenza audio/video;
- informazioni visualizzate stillo schermo del proprio PC;
- informazioni contenute su documenti cartacei esposti in prossimità della postazione di lavoro.

Allorquando si effettuino conferenze audio/video, si raccomanda di rendere note con chiarezza tutte le persone presenti. (Per la conduzione di conferenze audio/ video è preferibile utilizzare strumenti diffusi e consolidati come, ad esempio, Skype - https://www.skype.com/it/).

Evitare in generale che vengano effettuate fotografie, registrazioni video e registrazioni audio che rivelino, in tutto o in parte, qualsiasi aspetto della postazione di lavoro: persona in attività di lavoro agile, modello di computer utilizzato, contenuti visualizzati stillo scherno, contenuti stampati su documenti cartacei, conversazioni telefoniche. etc.

Limitare in generale il tempo di permanenza presso la postazione di qualsiasi documento cartaceo di lavoro, compresi quelli stampati direttamente presso il proprio domicilio, al tempo strettamente necessario alle relative attività di lavorazione/consultazione. Non appena saranno completate tali attività, qualora sia necessario custodire alcuni documenti cartacei, trasferirli nell'armadio, cassetto o altro contenitore munito di serratura, appositamente predisposto presso il proprio domicilio. Procedere quindi, subito dopo, con la completa distruzione dei documenti che non necessitano di essere custoditi. Nell'applicare la presente raccomandazione, gestire con priorità i casi in cui i documenti cartacei contengano anche dati personali e/o segreti d'ufficio.

Comunicare, senza ritardo, scrivendo al responsabile dei dati personali di Azienda Calabria Lavoro (*stefania.campagna@aziendacalabrialavoro.com*), ogni tipo di evento anomalo e/o incidente di sicurezza da cui potrebbe derivare una violazione di dati personali. A questo indirizzo non devono essere effettuate richieste di supporto e/ o chiarimenti. La segnalazione deve pervenire dall'indirizzo mail istituzionale del dipendente e per conoscenza al Direttore Generale.

FASE 3 - RIORDINO DELLA POSTAZION E DI LAVORO (CHECK-OUT)

Al termine della giornata lavorativa, assicurarsi di cestinare tutti i documenti/ file di lavoro rimasti memorizzati sul proprio PC. Qualora sia necessario custodire alcuni documenti/ file, procedere con l'upload degli stessi verso le opportune applicazioni informatiche e/o specifici file repnsitory eventualmente predisposti dall'Ente (si consiglia di adoperare la funzioone "*valigetta*" dal proprio account *Zimbra*). Procedere quindi, dopo tale periodo di lavorazione, con la completa cancellazione dal PC di tutti i documenti / file trattati nell'ambito dell'attività lavorative giornaliere.

Al termine della giornata lavorativa, assicurarsi di cestinare tutti i documenti cartacei di lavoro rimasti esposti presso la postazione di lavoro. Qualora sia necessario custodire alcuni documenti cartacei, trasferirli nell'armadio, cassetto o altro contenitore munito di serratura, appositamente predisposto presso il proprio domicilio. Procedere quindi, subito dopo, con la completa distruzione dei documenti che non necessitano di essere custoditi.

Al termina della giornata lavorativa, assicurarsi infine di spegnere il PC, oppure, nel caso in cui sia utilizzato da altri familiari o conviventi, assicurarsi di disconnettere semplicemente il proprio account.