Regione Calabria

Dipartimento Presidenza

DIREZIONE GENERALE

Prot. n.° 118750
del 25/03/2020

Ai **Dipartimenti Regionali** e alle **Strutture Equiparate**
della Giunta Regionale
Loro Sedi

A **Tutti i Dipendenti regionali**

e, p.c.
Al **Presidente della Giunta Regionale**

Oggetto: **Lavoro Agile (Smart Working)**
Raccomandazioni di sicurezza nell'utilizzo di informazioni e strumenti tecnologici

Viste le circolari:

- n. 103846 del 09.03.2020;
- n. 105026 del 10.03.2020;
- n. 107578 del 12.03.2020;
- n. 107674 del 12.03.2020;
- n. 110523 del 16.03.2020;
- n. 110656 del 16.03.2020;
- n.117919 del 24.03.2020;

con la presente, 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 saranno descritte in funzione delle 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).

Nel dettaglio, si tratta di adottare le raccomandazioni di sicurezza, per come descritto di seguito.

Cittadella Regionale, Viale Europa -Loc. Germaneto – 88100Catanzaro
☎+39 0961 856296 ✉f.varone@regione.calabria.itPEC dipartimento.presidenza@pec.regione.calabria.it

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

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

1.2. Verificare che il sistema operativo del proprio PC sia aggiornato all'ultima versione disponibile. (*L'aggiornamento del sistema operativo può essere verificato in Windows 10, accedendo a "Impostazioni > Aggiornamento e sicurezza > Windows Update". Per altri sistemi operativi consultare invece le relative guide utente*).

1.3. Verificare che sul proprio PC sia installato e attivato un antivirus aggiornato all'ultima versione disponibile. (*L'attivazione e l'aggiornamento di Windows Defender Antivirus, integrato in Windows 10, possono essere verificati accedendo a "Impostazioni > Aggiornamento e sicurezza > Sicurezza di Windows > Protezione da virus e minacce". Per altri antivirus consultare invece le relative guide utente*).

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

1.5. Verificare la robustezza delle diverse password utilizzate per accedere al proprio PC e alle applicazioni informatiche dell'Ente. Nel dettaglio, una 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 (*Nel caso della password del proprio PC si raccomanda il rinnovo settimanale*).

1.6. Nel caso in cui occorra trattare 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 armadio, cassetto o altro contenitore munito di serratura, per la loro custodia.

FASE 2 – UTILIZZO DELLA POSTAZIONE DI LAVORO

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

2.2. 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.
(*Tale operazione può essere eseguita in Windows 10 premendo contemporaneamente i tasti WIN+L sulla tastiera. Per altri sistemi operativi consultare invece le relative guide utente*).

2.3. 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 repository predisposti dall'Ente. Procedere quindi, dopo il 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 i casi in cui i documenti/file contengano anche dati personali e/o segreti d'ufficio.

2.4. 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 dati 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.

2.5. Prima di dar seguito ad ogni richiesta di informazioni, 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.

2.6. 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 sullo schermo del proprio PC;
- informazioni contenute su documenti cartacei esposti in prossimità della postazione di lavoro.

2.7. 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/).

2.8. 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 agile working, modello di computer utilizzato, contenuti visualizzati sullo schermo, contenuti stampati su documenti cartacei, conversazioni telefoniche, etc.

2.9. 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.

2.10. Comunicare, senza ritardo, scrivendo a rpd@pec.regione.calabria.it, 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 pec del settore di appartenenza pertanto deve essere concordata col dirigente.

FASE 3 – RIORDINO DELLA POSTAZIONE DI LAVORO (CHECK-OUT)

3.1. Al termine della giornata lavorativa, assicurarsi di gestire 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 repository predisposti dall'Ente. Procedere quindi, subito dopo, con la completa cancellazione dal pc di tutti i documenti/file trattati nell'ambito delle attività lavorative giornaliere.

3.2. Al termine della giornata lavorativa, assicurarsi di gestire 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.

3.3. Al termine 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.
(L'operazione di disconnessione del proprio account può essere eseguita in Windows 10 facendo clic sul pulsante Start, successivamente sul pulsante con il simbolo del proprio account (sulla sinistra dello schermo) ed infine sulla voce Disconnetti.
Per altri sistemi operativi consultare invece le relative guide utente.)

IL RESPONSABILE DELLA PROTEZIONE DATI
(Avv. Angela Stellato)

IL DIRIGENTE
(Dott. Fortunato Varone)