Allegato A

INFORMATIVA PER L'ACCESSO ALLA RETE PCM IN LAVORO AGILE

Testo dell'informativa

(**Aut. Dotazione – V.4.0)**

L'Amministrazione ha avviato da tempo un processo di trasformazione del posto di lavoro digitale per consentire l'esecuzione delle attività istituzionali in modalità agile, utilizzando strumenti di comunicazione e collaborazione in modalità "online" (Internet) e diversi metodi di accesso remoto alle risorse interne (applicazioni, cartelle condivise, ecc..). Ciò consente all'organizzazione di poter estendere i propri servizi oltre i confini della rete interna e oltre i limiti di una specifica Postazione di Lavoro (Desktop, Portatile, Telefono, Tablet). Oltre agli strumenti di collaborazione e comunicazione (Posta Elettronica, Videoconferenza, Condivisione File, Chat, Telefono, ecc..) disponibili sempre, in ogni luogo, e mediante qualsiasi dispositivo, l'Amministrazione valuta ed autorizza, caso per caso, la soluzione migliore da adottare tra le seguenti:

a) assegnazione di computer portatili con credenziali VPN-NPA (Virtual Private Network/ Network Private Access), router e SIM dati, per l'accesso a internet e per l'eventuale utilizzo degli applicativi interni della Presidenza del Consiglio dei ministri. In questo caso, l'Amministrazione, salvo sussistano motivate esigenze organizzative e/o insormontabili problematiche di tipo tecnico, provvede, anche ai fini di un razionale e flessibile utilizzo delle risorse ed in attuazione del piano di ammodernamento delle dotazioni informatiche, alla installazione presso la postazione del dipendente di una dock-station per l'utilizzo del laptop assegnato anche come postazione di lavoro fissa e per la connessione degli accessori [schermo, tastiera e mouse] e delle periferiche già in uso, ed infine al ritiro della postazione desktop assegnata. L'Amministrazione avrà la possibilità di procedere al blocco preventivo delle stesse in tutti i casi di compromissione rilevati anche ove non avesse la disponibilità fisica delle postazioni;

b) assegnazione di credenziali e profili di accesso remoto di tipo NPA, con l'applicazione di adeguate e vincolanti misure di sicurezza verificate ad ogni accesso (MFA), nel caso di utilizzo di postazioni informatiche e connessione dati, diverse da quelle dell'amministrazione, che sono nella disponibilità del dipendente.

Saranno infine messe a disposizione dei dipendenti modalità di comunicazione unificata, fissa e mobile, per la massima reperibilità, indipendentemente dalla posizione fisica. A tale scopo verranno utilizzati tutti i sistemi di collaborazione e comunicazione di cui la Presidenza del Consiglio dei ministri dispone.

ACCESSO VPN/NPA alla rete PCM

Il dipendente ammesso al lavoro agile ottiene l'accesso VPN/NPA alla rete della Presidenza del Consiglio dei ministri, con la consegna delle relative credenziali di accesso.

L'accesso è finalizzato alla esecuzione, in modalità agile, delle attività istituzionali concordate tra il dipendente e il superiore gerarchico nel progetto individuale di lavoro agile.

Le condizioni per l'accesso, che il dipendente si impegna a rispettare, sono le seguenti:

- L'accesso sarà effettuato per mezzo del computer portatile fornito dalla PCM. L'utente si impegna ad usare il portatile assegnato esclusivamente per le attività di ufficio.

- L'utente si impegna a custodire il portatile assegnato con la massima cura e diligenza e a non consentirne l'uso a terzi.
  In particolare:

- a non lasciare il portatile assegnato incustodito in luoghi accessibili al pubblico;
- ad utilizzare le proprie credenziali di accesso alla macchina e a configurare il salvaschermo in modo che blocchi la sessione dopo un periodo massimo di 10 minuti di non uso;
- a verificare che la connessione avvenga secondo le modalità e verso gli indirizzi indicati dal manuale d'uso come corretti e affidabili;
- a non manomettere l'antivirus fornito col portatile e a richiedere assistenza nel caso ritenga che l'antivirus non funzioni correttamente;
- a utilizzare l'account utente senza richiedere privilegi di amministratore della macchina;
- a mantenere il software di sistema aggiornato;
- a non installare software estraneo alle attività istituzionali; in particolare a non installare software per scambio di file "peer to peer".
- a non installare software di provenienza incerta, a non installare software pervenuto per mezzo di un messaggio di posta elettronica anche se proveniente da mittente conosciuto, ecc.
- a utilizzare le proprie credenziali esclusivamente per l'accesso agli strumenti istituzionali e a non utilizzare il proprio account di posta elettronica per la registrazione su siti internet, social network, ecc.

- In caso di compromissione del portatile, sarà cura dell'utente darne comunicazione all'Ufficio per l'informatica e la telematica – Servizio sistemi ed infrastrutture di Rete per l'immediata disabilitazione dell'accesso. Esempi non esaustivi di compromissione sono: smarrimento del portatile, uso del portatile da parte di terzi, sospetta infezione di virus informatici del portatile, ecc. La valutazione sull'entità della compromissione potrà essere effettuata dall'UIT. Al termine della situazione di compromissione, saranno emesse nuove credenziali di accesso.

- L'utente comunicherà, appena ne sia a conoscenza, all'UIT, ogni variazione del proprio status amministrativo, che comporti la cessazione del titolo ad usufruire del servizio VPN o di altri servizi informatici a cui è o sarà consentito l'accesso tramite le credenziali assegnate con la presente, ad es. per dimissioni, cambio di mansioni, ecc.

- L'utente è a conoscenza e autorizza che le attività svolte sulla rete durante la sessione VPN o NPA (cioè a VPN attiva) siano registrate sui sistemi informatici della PCM, e che sia possibile associare immediatamente e direttamente tali attività alla propria utenza individuale (nome e cognome). Ulteriori dettagli sulla registrazione delle attività possono essere forniti su richiesta dell'interessato.

- L'utente si impegna ad utilizzare l'accesso VPN/NPA per i soli fini per cui è stato concesso e/o in generale per fini istituzionali.

- L'utente si impegna a conservare le credenziali di accesso alla VPN/NPA (username; password; certificato) con la massima cura e a non divulgarle o consegnarle scientemente a terzi.

- L'utente si impegna a non divulgare a terzi alcuna informazione riguardo questa modalità di connessione. Le credenziali di accesso avranno una durata limitata al periodo del progetto in modalità agile. Sarà cura di ogni intestatario, qualora ne abbia titolo, richiederne il rinnovo prima della scadenza.

- La PCM, in caso di necessità e urgenza, potrà sospendere l'accesso VPN/NPA in qualsiasi momento anche senza preavviso. L'utente avrà comunque la possibilità di richiedere informazioni sullo stato di funzionamento del proprio accesso VPN.

- Nel caso di interventi di manutenzione relativi alle risorse in dotazione si dovranno seguire le usuali procedure di richiesta assistenza tramite il sistema di HELP DESK telefonando al n. 06/67794545 o inviando una mail a servicedesk@palazzochigi.it.

- L’utente si impegna a prendere visione dei seguenti documenti:

    - PROTOCOLLO PER L’UTILIZZO DEI SERVIZI INFORMATICI E TELEMATICI (disponibile sulla rete intranet, nella sezione “Servizi strumentali – Servizi ICT rete - Protocollo per l'utilizzo dei servizi informatici e telematici” - http://www.pcm.it//Strumentali/ICT/protocolloutilizzo.shtml);
    - ISTRUZIONI PER ACCEDERE ALLA VPN-PCM (disponibile sulla rete intranet, indirizzo http://www.pcm.it/Accoglienza/lavoroagile_salute.shtml)

  e a rispettare tutte le prescrizioni ivi riportate per l’accesso alle risorse tecnologiche e per l’uso dei servizi a cui è abilitato, nel pieno rispetto delle misure di sicurezza informatica della PCM.

L’autorizzazione all’accesso ai servizi di rete è consentita per tutta la durata del proprio accordo di lavoro agile. Ulteriori informazioni ed aggiornamenti saranno pubblicati su un’apposita area della Intranet dedicata al lavoro agile.