Ministero del Turismo

MINISTERO DEL TURISMO
REPUBBLICA ITALIANA

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

1. Premessa

L'utilizzo di sistemi Informatici ricevuti dall'Amministrazione ai fini dell'espletamento della propria mansione da locazioni remote esterne al perimetro dell'ordinaria sede di lavoro deve essere effettuato con la necessaria consapevolezza dei potenziali rischi sulla sicurezza dei sistemi informatici ricevuti prodotti dall'inosservanza di regole di comportamento messe in atto nell'attività in lavoro agile.

Il Ministero del Turismo, 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.

2. Rischi connessi a un utilizzo improprio delle credenziali di accesso.

L'accesso ai sistemi informatici forniti dall'Amministrazione prevede l'utilizzo di credenziali (nome utente e password) devono essere adeguatamente custodite.

In particolare, 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 basarsi su parole comuni, cioè reperibili in rete, e non devono essere facilmente associabili alla persona;

 devono sempre contenere caratteri maiuscoli e minuscoli;

 devono essere cambiate con cadenza trimestrale, a meno di conseguente blocco dell'account.

3. 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, di sicurezza e del sistema antivirus.

4. Rischi correlati all'utilizzo della casella di posta istituzionale

I messaggi presenti nella casella di posta elettronica istituzionale possono contenere informazioni riservate o dati personali rispetto ai quali devono essere poste in essere tutte le attenzioni necessarie al fine di 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 al punto 2;

- 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".

5. Rischi derivanti da comportamenti impropri.

Si raccomanda attenzione nella gestione e nella custodia delle informazioni e dei dati personali trattati durante l'espletamento dell'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 o bloccato lo schermo;

- impostare la richiesta di credenziali di accesso all'avvio del PC;

- in caso di utilizzo di dispositivi portatili, non esporre questi ultimi a rischio di furto o smarrimento.

6. Conclusione

Si ribadisce, in particolare:

-Al fine di ridurre il potenziale pericolo di attacchi informatici (virus worm, trojan, etc) è obbligatorio accertarsi della presenza e dell'attivazione sul proprio computer di 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 Sistema Operativo del sistema informatico assegnato installando le patch di sicurezza che periodicamente vengono distribuite dal produttore del Sistema Operativo.