Norme di comportamento del dipendente nelle attività lavorative svolte nella modalità di lavoro agile

Portiamo a conoscenza del personale che svolge la propria attività in modalità di lavoro agile le raccomandazioni elaborate da Cert-PA di AgID per il rispetto delle misure minime di sicurezza informatica per le pubbliche amministrazioni fissate dalla circolare 17 marzo 2017, n. 1 che devono essere garantite anche dal personale che svolge la propria attività lavorativa da remoto:

1. Segui prioritariamente le policy e le raccomandazioni dettate dalla tua Amministrazione;
2. Utilizza i sistemi operativi per i quali attualmente è garantito il supporto (non utilizzare, ad esempio, macchine con sistema operativo windows XP o windows 7 di cui microsoft ha terminato il supporto);
3. Effettua costantemente gli aggiornamenti di sicurezza del tuo sistema operativo;
4. Assicurati che i software di protezione del tuo sistema operativo (Firewall, Antivirus, ecc) siano abilitati e costantemente aggiornati;
5. Assicurati che gli accessi al sistema operativo siano protetti da una password sicura di almeno 8 caratteri contenente almeno una lettera maiuscola, un numero ed un carattere speciale;
6. Non installare software proveniente da fonti/repository non ufficiali
7. Blocca l'accesso al sistema e/o configura la modalità di blocco automatico quando ti allontani dalla postazione di lavoro;
8. Non cliccare su link o allegati contenuti in email sospette;
9. Utilizza l'accesso a connessioni Wi-Fi adeguatamente protette;
10. Collegati a dispositivi mobili (pen-drive, hdd-esterno, etc) di cui conosci la provenienza (nuovi, già utilizzati, forniti dalla tua Amministrazione);
11. Effettua sempre il log-out dai servizi/portali utilizzati dopo che hai concluso la tua sessione lavorativa.

Si coglie l'occasione per dare le seguenti ulteriori disposizioni:

- Nel caso in cui utilizzi un PC personale per svolgere l'attività lavorativa, prima del suo primo utilizzo, installa un buon antivirus e fai una accurata scansione preventiva per rimuovere qualunque software malevolo;
- Non memorizzare sui dispositivi le password di accesso alle piattaforme ed ai sistemi utilizzati per il lavoro a distanza;
- Non memorizzare sul client di posta elettronica le credenziali di accesso alle caselle istituzionali;
- Accertati di aver impostato una password sicura sul router utilizzato per l'accesso ad Internet (accertati di non aver lasciato la password di default proposta dal costruttore e nota a qualunque malintenzionato);
- Se utilizzi una connessione wifi, accertati di adottare una password sicura per il suo accesso (mai lasciare accessi liberi alla rete wifi).

Il Dirigente Scolastico
Titolare del Trattamento
(Prof. Roberto Maniscalco)

Documento informatico firmato digitalmente ai sensi del D.Lgs 82/2005 s.m.i.
e norme collegate, il quale sostituisce il documento cartaceo e la firma autografa