INFORMATIVA SULLE REGOLE DI COMPORTAMENTO NELL'UTILIZZO DELLE DOTAZIONI INFORMATICHE DURANTE IL LAVORO AGILE

L'utilizzo di sistemi informatici utilizzati per lo svolgimento delle proprie mansioni da postazioni remote esterne al perimetro dell'Ateneo, deve essere effettuato con la necessaria consapevolezza dei potenziali rischi sulla sicurezza dei sistemi aziendali.

In particolare, si richiama l'attenzione sulle seguenti regole di comportamento necessarie a garantire la corretta operatività per l'accesso ai sistemi dell'Ateneo da remoto nel rispetto dei livelli di sicurezza necessari.

Postazione di lavoro e collegamento alla rete internet

L'apparecchiatura utilizzata nell'attività lavorativa deve essere sempre dotata di un sistema operativo standard aggiornato secondo le indicazioni del produttore e di software antivirus costantemente aggiornato.

I sistemi operativi della propria postazione di lavoro devono essere aggiornati secondo le indicazioni ricevute automaticamente dalle società produttrici. Un sistema operativo aggiornato garantisce l'immunità da virus e worm che potrebbero prendere il controllo della propria stazione di lavoro. A tal proposito è proibito disabilitare gli aggiornamenti automatici del sistema operativo e dei sistemi antivirus installati.

È necessario assicurarsi della disponibilità di un collegamento alla rete internet attivo e con capacità di banda sufficiente a garantire continuità di collegamento *anche in caso di più soggetti utilizzanti collegamenti contemporanei nella stessa abitazione.*

In caso di utilizzo della postazione di lavoro da parte di più soggetti è necessario utilizzare un account dedicato ai collegamenti per lo svolgimento delle prestazioni lavorative separato da altre utenze di tipo familiare.

Riservatezza della password di accesso ai servizi

L'accesso ai sistemi e servizi informatici dell'Ateneo prevede l'utilizzo di credenziali (nome utente e password gestite dal sistema D.S.A. (directory service d'Ateneo) che devono essere adeguatamente custodite in luogo sicuro e non devono essere divulgate ad altri per nessuna ragione.

Password all'accensione e blocco schermo con password

È necessario assicurare che il dispositivo utilizzato per l'erogazione delle prestazioni lavorative abbia impostata una password di accensione e di blocco schermo al fine di evitare che soggetti terzi possano entrare in contatto con ambienti e comunicazioni aziendali in caso di abbandono temporaneo della postazione di lavoro.

Consenso, in caso di necessità, ad una verifica preliminare da parte dello staff tecnico informatico

Su richiesta del supporto tecnico e sotto il controllo del lavoratore, il personale dell'Ateneo incaricato per la gestione dei servizi informatici (CSIA) potrà richiedere al dipendente il controllo da remoto del dispositivo utilizzato per il lavoro agile ai fini dello svolgimento di attività di troubleshooting per la verifica relativa alla correttezza delle impostazioni di sicurezza e per la risoluzione di eventuali problemi tecnici.