Allegato B
alla sottosezione del PIAO relativa all' *Organizzazione del Lavoro Agile* 2024-2026

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

L'utilizzo di sistemi Informatici acceduti nell'espletamento della propria mansione da locazioni remote esterne al perimetro aziendale deve essere effettuato con la necessaria consapevolezza dei potenziali rischi sulla sicurezza dei sistemi aziendali prodotti dall'inosservanza di regole di comportamento messe in atto nell'attività in lavoro agile.
Asl3, 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 e delle misure di sicurezza tecnica contenute nelle procedure aziendali in materia di utilizzazione delle dotazioni informatiche e della posta elettronica aziendale, per gli aspetti compatibili, con particolare riguardo all'uso della connessione VPN per l'attività in lavoro agile.

Rischi connessi ad un utilizzo improprio delle credenziali di accesso.
L'accesso ai sistemi informatici Aziendali tramite connessione remota VPN è consentita solo all'interno del territorio italiano. È consentito l'accesso da alcuni paesi dell'U.E. solo in via eccezionale e dietro specifica verifica e autorizzazione.

L'accesso ai sistemi informatici aziendali prevede l'utilizzo di credenziali (nome utente e password, ad personam), necessarie per accedere ai sistemi aziendali e come tali devono essere adeguatamente custodite.
In particolare per 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 essere banali, cioè reperibili in rete, non facilmente associabili alla persona, non essere ripetizione della *login* o una permutazione ciclica della stessa, né una stringa di caratteri contigui della tastiera.
- devono sempre contenere caratteri maiuscoli e minuscoli;
- devono essere cambiate con cadenza trimestrale, a meno di conseguente blocco dell'account, evitando il riutilizzo di chiavi già adottate nei 12 mesi precedenti;
- al cambio password non possono essere utilizzate le ultime 4 impostate.

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. È inoltre da evitare l'utilizzo di sistemi operativi obsoleti. L'accesso ai sistemi aziendali è consentito esclusivamente da computer dotati dei seguenti sistemi operativi:

- Microsoft Windows Versione 7
- Microsoft Windows Versione 8 e 8.1
- Microsoft Windows Versione 10 o successive
- Mac OS X o Linux (previa verifica tecnica della S.C. Sistemi Informativi Aziendali)

L'apparecchiatura utilizzata nell'attività lavorativa deve essere sempre dotata di un software antivirus costantemente aggiornato. A tal proposito, si segnala che le più recenti versioni dei sistemi operativi Microsoft mettono a

disposizione o integrano strumenti antivirus quali Microsoft Security Essentials e Microsoft Windows Defender dei quali, comunque, si raccomanda di verificare periodicamente il loro regolare funzionamento e aggiornamento.

Rischi correlati all'utilizzo della casella di posta aziendale.
I messaggi presenti nella casella di posta elettronica aziendale possono contenere informazioni riservate o dati personali per i quali devono essere poste in essere tutte le attenzioni necessarie ad 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;
- → 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*".

Rischi derivanti da comportamenti impropri.
Si raccomanda attenzione nella custodia di informazioni aziendali e dati personali utilizzati durante l'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 del sistema operativo o bloccato lo schermo (CTRL+ALT+CANC e poi BLOCCA);
- → impostare la richiesta di credenziali di accesso al sistema operativo all'avvio del PC;
- → in caso di collegamento a terminal server RDP (Desktop Remoto) o connessione VPN, non utilizzare altro software presente sulla propria macchina, in particolare browser e client mail.
- → in caso di utilizzo di dispositivi portatili, non esporre questi ultimi a rischio di furto o smarrimento.

Riepilogo.

Requisiti minimi necessari per il collegamento telematico alla Rete di Asl3:

- → Collegamento solo da dispositivi all'interno del territorio italiano (solo in via eccezionale e dietro specifica verifica e autorizzazione da alcuni ristretti Paesi dell'U.E.);
- → Personal computer dotato di sistema operativo Microsoft Windows 7, 8, 10 o successive con browser Microsoft EDGE o CHROME, ovvero Sistema Operativo Mac OS X o Linux previa verifica dei requisiti tecnici da parte della S.C. Sistemi Informativi Aziendali.
- → Collegamento a Internet attraverso linea di connessione dati ADSL o fibra con banda minima pari ad almeno 10 Mbps in download, in alternativa è consentito l'utilizzo di tecnologie di connessione dati basate su rete cellulare, in tal caso i protocolli di collegamento dati dovranno garantire una velocità minima di connessione pari a 10 Mbps in download su tecnologie UMTS, HSDPA, LTE o 5G.
- → Al fine di ridurre il potenziale pericolo di attacchi informatici (virus worm, trojan, etc.) è obbligatorio:
    - attivare sul proprio computer 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 proprio Sistema Operativo installando le patch di sicurezza che periodicamente vengono distribuite dal produttore del Sistema Operativo.

Per ricevuta ed accettazione

Data

Il Dipendente _____