ISTITUTO COMPRENSIVO STATALE "ARTURO BENEDETTI MICHELANGELI"
Via Dante Alighieri , 10 – 20084 LACCHIARELLA (MI) Cod. Meccanografico MIIC88200X –
Cod. Fiscale 80124710155 ☎ 02/9008096 - 🖷 02/90030428 MIIC88200X@pec.istruzione.it

ALLEGATO TECNICO all'ACCORDO INDIVIDUALE LAVORO da REMOTO

Requisiti minimi di sicurezza per i dispositivi utilizzati nel lavoro da remoto

1. Oggetto e finalità

Il presente allegato definisce i requisiti tecnici minimi che devono essere rispettati dal dispositivo informatico utilizzato dal dipendente per lo svolgimento della prestazione lavorativa in modalità da remoto, al fine di garantire:

- **la sicurezza dei dati trattati**
- **la protezione delle informazioni dell'Istituto**
- **la conformità alle normative vigenti (GDPR, D.Lgs. 196/2003, Linee guida AGID)**
- **la continuità operativa e la prevenzione di accessi non autorizzati**

Il dipendente è responsabile del rispetto dei requisiti indicati nel presente documento.

2. Requisiti del dispositivo

2.1 Account e accesso

- **Il dispositivo deve essere utilizzato tramite account personale non condiviso.**
- **L'accesso deve essere protetto da password robusta o autenticazione forte.**

2.2 Sistema operativo

- **Il sistema operativo deve essere supportato dal produttore e aggiornato.**
- **Gli aggiornamenti automatici devono essere attivi.**

2.3 Software applicativo

- **Devono essere aggiornati: browser, suite Office, applicazioni di lavoro, driver.**
- **È vietato installare software pirata o non autorizzato.**

2.4 Protezione da malware

- **Deve essere presente un antivirus attivo e aggiornato.**

- **Il firewall deve essere abilitato.**

2.5 Sicurezza della connessione

- **La connessione deve avvenire tramite rete Wi-Fi protetta (WPA2 o superiore).**
- **È vietato l'uso di reti pubbliche o non protette.**
- **Il router deve avere password amministratore modificata e firmware aggiornato.**

2.6 Protezione dei dati

- **I documenti dell'Istituto devono essere trattati solo tramite piattaforme istituzionali.**
- **È vietato salvare dati su cloud personali, USB non protette o cartelle condivise.**
- **È raccomandata la crittografia del disco.**

2.7 Accesso ai sistemi dell'Istituto

- **L'accesso deve avvenire tramite credenziali istituzionali e connessioni sicure.**
- **Le credenziali non devono essere salvate in chiaro o condivise.**

2.8 Backup e conservazione

- **I documenti devono essere conservati solo nei sistemi autorizzati.**
- **È vietato effettuare backup locali non protetti.**

2.9 Software di controllo remoto

- **È vietato l'uso di software di controllo remoto non autorizzati (TeamViewer, AnyDesk).**
- **Eventuali strumenti di assistenza devono essere approvati dall'Amministrazione.**