Allegato 3

INFORMATIVA IN MATERIA DI SICUREZZA DI UTILIZZO DELLA RETE, DEI DISPOSITIVI ELETTRONICI E DEI DATI

Il dipendente è tenuto a prestare la massima attenzione nella gestione dei dati personali di terzi, che sia stato autorizzato a trattare sulla base dell'informativa pubblicata sul sito https://unige.it/ateneo/privacy, attenendosi alle prescrizioni del Regolamento dell'Università degli studi di Genova in materia di trattamento dei dati personali (https://unige.it/sites/contenuti.unige.it/files/documents/Regolamento_trattamento_dati_personali.pdf) e alle ulteriori indicazioni fornite sul sito di Ateneo relativo alla privacy, ivi incluse le disposizioni in materia di *data breach* (violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione o l'accesso ai dati personali trasmessi, conservati o, comunque, trattati dall'Università).

Il dipendente è tenuto a preservare la sicurezza del sistema informativo universitario e delle informazioni dell'ente. I dispositivi utilizzati per le attività lavorative devono essere usati con la massima diligenza, avendo cura di adottare gli accorgimenti e le misure utili ad evitare la manomissione involontaria e/o la sottrazione di dati, nonché la rivelazione di informazioni confidenziali e riservate a persone non autorizzate.

In particolare

- Al fine di ridurre il rischio di compromettere Il dispositivo personale impiegato per lavorare da remoto dovrebbe possibilmente non essere in uso condiviso con altre persone (ad es. altri familiari) e nell'impossibilità di ciò, chi lo utilizza in condivisione non dovrebbe avere credenziali amministrative (per impedire che possa essere installato da altri, anche involontariamente, *software* malevolo);
- il sistema operativo deve essere aggiornato regolarmente e con tutti i più recenti aggiornamenti di sicurezza;
- l'antivirus deve essere aggiornato almeno quotidianamente e deve essere attivo, come pure il *firewall* personale del sistema operativo;
- prima di iniziare l'attività lavorativa bisogna attivare la connessione VPN per evitare che i dati in transito sulla rete internet possano essere osservati (le istruzioni per l'installazione e configurazione della VPN sono sul sito CeDIA https://cedia.unige.it/istruzioni-vpn);
- una volta accertata l'attivazione della VPN non operare direttamente sul proprio dispositivo ma accedere in remote desktop al PC in ufficio (che deve rimanere acceso) e operare con i programmi da esso;
- evitare il più possibile di trasportare documenti di lavoro sul proprio PC;
- non aprire allegati all'interno di email ricevute (anche sulla casella personale) ma, salvarli su disco e sottoporli a scansione antivirus prima di aprirli;
- evitare di cliccare su *link* contenuti nelle email (anche sulla casella personale) ma copiarli ed esaminarli per individuare anomalie nell'indirizzo prima di avviarli nel browser (spesso il *link* nella mail appare diverso da quello che si va effettivamente a visitare);
- se si notasse un comportamento anomalo del PC, scollegarlo immediatamente dalla rete e segnalare l'evento a CeDIA per le necessarie investigazioni.

A garanzia della riservatezza, l'integrità e la disponibilità delle informazioni trattate mediante le risorse aziendali, il dipendente è tenuto a segnalare qualsiasi evento anomalo o dubbio,

potenzialmente in grado di compromettere la sicurezza informatica delle informazioni, alla *mail* assistenza@unige.it.