ISTRUZIONI PER IL TRATTAMENTO DATI CITTADINI E UTENTI MEDIANTE USO DELLA RETE INFORMATICA E DEI SERVIZI ICT PER LO SMART WORKING NEL PERIODO DELL'EMERGENZA SANITARIA DA COVID-19

A fronte dell'emergenza sanitaria da COVID-19 (coronavirus), l'attivazione del lavoro agile (c.d. smart working), inteso come modalità di esecuzione del rapporto di lavoro subordinato caratterizzato dall'assenza di vincoli orari o spaziali e un'organizzazione per fasi, cicli e obiettivi, stabilita anche in deroga all'accordo tra dipendente e datore di lavoro, impone:

- **l'uso di servizi e soluzioni tecnologie ICT per i lavoratori delle PA.**

Questi ultimi possono utilizzare **anche i propri dispositivi** per effettuare la prestazione lavorativa in modalità agile.

L'amministrazione, alla data odierna, ha già adottato una serie di MISURE, per attivare il lavoro agile, tra cui:

- **Atto di macro organizzazione** nell'ambito della gestione del rapporto di lavoro e/o **altra tipologia di atto (Direttiva/Linea guida**) contenente regole dello smart working straordinario;
- **Circolari** a tutti i Dirigenti/P.O. e a tutti i dipendenti sugli obblighi di segnalazione e modalità operative;
- **Modulistica** utilizzabile dai lavoratori e dal datore di lavoro, compresa l'informativa ai sensi della legge 81/2017 sulla salute e la sicurezza nei luoghi di lavoro;
- **Informative** ai lavoratori in ordine al trattamento dei loro dati personali durante lo smart working straordinario;

A queste misure, **SI RACCOMANDA** di aggiunge anche le odierne **ISTRUZIONI**, da diramare a tutti i dipendenti tramite comunicazione personale attraverso canale adeguato per garantire una conoscenza effettiva da parte dei destinatari.

***

ISTRUZIONI

in ordine al trattamento dei dati personali dei cittadini e degli utenti, mediante uso della rete informatica e dei servizi ICT per lo smart working in deroga (o smart working straordinario) nel periodo dell'emergenza sanitaria da COVID-19 (coronavirus).

Fermo restando che ogni dipendente-utente che effettua lo smart working è responsabile, disciplinarmente, civilmente e, se del caso, penalmente del corretto uso delle della rete informatica e delle risorse informatiche, nonchè dei servizi/programmi ai quali ha accesso, valgono i seguenti divieti.

1. **Durante il periodo dell'emergenza sanitaria, e nell'ambito dello smart working c.d. straordinario, sono vietati, nell'uso della RETE, i seguenti comportamenti:**

- comunicare ad altri, o comunque rendere disponibili ad altri, i dati relativi al proprio account di rete (username e password). la password è segreta, strettamente personale, non deve essere divulgata e deve essere debitamente conservata
- conseguire l'accesso non autorizzato a risorse di rete interne alla rete dell'amministrazione

- conseguire l'accesso non autorizzato a risorse di rete esterne alla rete dell'amministrazione, tramite la stessa alla rete dell'amministrazione
- agire deliberatamente con attività che influenzino negativamente la regolare operatività della rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti
- effettuare trasferimenti non autorizzati di informazioni (software, dati, ecc).
- installare, eseguire o diffondere su qualunque computer e sulla rete, programmi destinati a danneggiare o sovraccaricare i sistemi o la rete (ad es. virus, cavalli di troia, worms, spamming della posta elettronica).
- installare o eseguire programmi software non autorizzati o non compatibili con l'attività istituzionale
- cancellare, copiare o asportare programmi software per scopi personali.
- installare componenti hardware non compatibili con l'attività istituzionale
- installare componenti hardware non acquistati dall'amministrazione e non di proprietà dell'amministrazione non autorizzati
- rimuovere, danneggiare o asportare componenti hardware
- utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività di altri utenti, per leggere, copiare o cancellare files e software di altri utenti.
- utilizzare software visualizzatori di pacchetti tcp/ip (sniffer), software di intercettazione di tastiera (keygrabber), software di decodifica password (cracker) e più in generale software rivolti alla violazione della sicurezza del sistema e della privacy
- usare l'anonimato o servirsi di risorse che consentano di restare anonimi.
- inserire password locali alle risorse informatiche assegnate (come ad esempio password che non rendano accessibile il computer agli amministratori di rete), se non espressamente autorizzati e debitamente comunicate al servizio sistemi informativi
- abbandonare il posto di lavoro lasciandolo senza protezione da accessi non autorizzati.

L'amministrazione adotta, quale misura di sicurezza e di protezione dei dati, l'obbligatoria **registrazione, in appositi file riconducibili ad un account di rete, di ogni attività compiuta nella rete informatica. L'amministrazione si riserva di effettuare, per fini legati alla sicurezza del sistema informatico, il controllo della posta e della navigazione in internet** e, in tale caso, prima di iniziare il trattamento, a tutela del dipendente, comunicherà gli strumenti e i modi di trattamento effettuati. In ogni caso, i file contenenti le registrazioni possono essere soggetti a trattamento solo per fini istituzionali, per attività di monitoraggio e controllo e possono essere messi a disposizione dell'autorità giudiziaria in caso di accertata violazione della normativa vigente.

2. **Durante il periodo di smart working in deroga nell'ambito dell'emergenza sanitaria sono vietati, nell'uso INTERNET, i seguenti comportamenti:**

- l'accesso a siti inappropriati (esempio siti pornografici, di intrattenimento, ecc.).
- lo scaricamento (download) di software e di file non necessari all'attività istituzionale.
- utilizzare programmi per la condivisione e lo scambio di file in modalità peer to peer.
- accedere a flussi in streaming audio/video da internet per scopi non istituzionali;
- un uso di internet che possa in qualche modo recare qualsiasi danno all'amministrazione o a terzi.

3. **Durante il periodo di smart working in deroga nell'ambito dell'emergenza sanitaria sono vietati, nell'uso della POSTA ELETTRONICA i seguenti comportamenti:**

- la trasmissione a mezzo di posta elettronica di dati sensibili, confidenziali e personali di alcun genere, salvo i casi espressamente previsti dalla normativa vigente in materia di protezione dei dati personali (Reg. UE 2016/679 e d.lgs. 196 del 30/6/2003).

- la comunicazione all'esterno, senza preventiva autorizzazione dell'amministrazione responsabile del trattamento, della documentazione elettronica che viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto.
- la partecipazione a dibattiti, forum o mailing-list, salvo diversa ed esplicita autorizzazione
- l'apertura di allegati ai messaggi di posta elettronica senza il previo accertamento dell'identità del mittente
- inviare tramite posta elettronica user-id, password, configurazioni della rete interna, indirizzi e nomi dei sistemi informatici
- inoltrare "catene" di posta elettronica (catene di s.antonio e simili), anche se afferenti a presunti problemi di sicurezza.
- inoltrare messaggi di posta elettronica all'interno dell'amministrazione a contenenti allegati di notevole dimensione (ad esempio di dimensioni superiori a 2 mbyte).
- un uso di posta elettronica che possa in qualche modo recare qualsiasi danno al all'amministrazione o a terzi.

4. Durante il periodo di smart working in deroga nell'ambito dell'emergenza sanitaria sono vietati, nell'uso dei DISPOSITIVI portatili, i seguenti comportamenti:

- utilizzare un pc NON munito di software antivirus e di software firewall, e non controllare periodicamente i relativi aggiornamenti.
- l'utilizzo di reti private virtuali (VPN) di qualsiasi tipologia, fatta eccezione per le VPN istituzionali e/o comunicate/autorizzate dall'amministrazione medesima;
- non effettuare l'aggiornamento continuo degli applicativi software e del sistema operativo, al fine di ridurre le vulnerabilita' informatiche;
- lasciare incustoditi i dispositivi (PC) portatili utilizzati all'esterno, per lo smart working, in caso di allontanamento;
- l'installazione di dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, dischi esterni, i-pod, telefoni, ecc.), se non con l'autorizzazione espressa dell'amministrazione.
- omettere di avvertire immediatamente l'amministrazione, nel caso in cui vengano rilevati virus o eventuali malfunzionamenti.
- omettere di spegnere ogni sera il dispositivo, tenuto conto che lasciare il dispositivo incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.
- omettere di attivare lo screensaver e di fare uso della relativa password.
- accesso ai dati e ai programmi da utilizzare per la gestione amministrativa presenti anche quando non si rende indispensabile ed indifferibile per esclusive necessità di funzionalità operativa dell'attività
- tenere comportamenti tali da aumentare il rischio di attacco al sistema informatico mediante virus o mediante ogni altro software aggressivo
- omettere di controllare il regolare funzionamento e l'aggiornamento periodico dei software installato, secondo le procedure previste
- omettere di seguire la seguente procedura, nel caso che il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente: a) sospendere ogni elaborazione in corso senza spegnere il computer; b) segnalare l'accaduto al Responsabile del Servizio Sistemi Informatici.

5. **Durante il periodo di smart working in deroga nell'ambito dell'emergenza sanitaria sono vietati, nell'uso dei <u>SUPPORTI MAGNETICI</u>, i seguenti comportamenti:**

- omettere di sottoporre ad un preventivo controllo ed alla relativa autorizzazione da parte del Responsabile del Servizio Sistemi Informatici e/o del suo staff tecnico, l'impiego di supporti magnetici riutilizzabili (hard drive esterni, chiavi USB, CD riscrivibili)
- utilizzare cd rom, cd riscrivibili chiavette usb di provenienza ignota
- omettere di custodire in archivi chiusi a chiave tutti i supporti riutilizzabili contenenti dati sensibili e giudiziari;
- omettere di trattare con particolare cautela e diligenza tutti i supporti magnetici riutilizzabili contenenti dati sensibili e giudiziari onde evitare che il loro contenuto possa essere recuperato tenuto conto che un soggetto esperto potrebbe recuperare i dati memorizzati anche dopo la loro cancellazione
- tutti i files di provenienza incerta, ancorché potenzialmente attinenti all'attività lavorativa, non devono essere utilizzati / installati / testati.
- omettere di consegnare all'Amministratore di Sistema per l'opportuna distruzione tutti i supporti magnetici riutilizzabili (hard drive esterni, chiavi USB, CD riscrivibili) obsoleti

Si raccomanda il rispetto delle regole contenute nelle presenti ISTRUZIONI per la sicurezza e la protezione dei dati dei cittadini e degli utenti durante lo smart working.