REGOLAMENTO per lo svolgimento della prestazione in modalità "lavoro agile" e "lavoro da remoto". ALLEGATO C). Disposizioni sull'utilizzo della dotazione informatica e telematica per il lavoro agile e da remoto.

Le presenti disposizioni riguardando il personale che, per effettuare la prestazione lavorativa in modalità agile o da remoto, mette a disposizione dispositivi di sua proprietà ovvero che utilizzi apparati dell'Ente, adottando comportamenti e misure adeguate per la protezione ai fini della sicurezza informatica, come previsto nel "DISCIPLINARE DI GESTIONE DEGLI STRUMENTI IT DELL'AUTORITÀ IDRICA TOSCANA E DI UTILIZZO DELLA POSTA ELETTRONICA E DI INTERNET" (Allegato n.2 al Decreto D.G. n.139 del 2021), nelle 11 raccomandazioni pubblicate da AgID il 17 marzo 2020 sul lavoro agile o da remoto, e nel vademecum "Buone pratiche di cyber hygene per i dipendenti delle Pubbliche Amministrazioni" allegato al protocollo 10755/2025 (scaricabile tramite il seguente link https://noipa.mef.gov.it/cl/web/guest/-/sicurezza-digitale-nella-pa-pubblicato-il-vademecum-dell-agenzia-per-la-cybersicurezza-nazionale?inheritRedirect=true).

Qualora la dotazione informatica e telematica per il lavoro agile o da remoto sia in tutto o in parte fornita dall'Ente al dipendente, lo stesso è incaricato della corretta custodia ed è responsabile del suo corretto utilizzo.
La dotazione completa è formata da un PC portatile, un dispositivo USB per la connessione dati, un telefono cellulare "smartphone".

Contestualmente alla consegna degli apparati sono forniti in dotazione di base i seguenti accessori:
Per il telefono:

- batteria
- carica batteria
- auricolare
- custodia
- SIM Card.

Per il computer portatile:

- Alimentatore
- tastiera
- mouse
- borsa

Per il dispositivo USB:

- SIM Card.

Tutto il materiale è assegnato per esclusivo uso lavorativo; non può essere ceduto a terzi a nessun titolo e per nessun motivo.
Nell'utilizzo degli apparati di proprietà dell'Ente il dipendente dovrà adottare la diligenza del buon padre di famiglia e gli accorgimenti per il corretto utilizzo che ne garantiscano la sicurezza individuale.

L'assegnatario è altresì responsabile del corretto utilizzo dell'apparato dal momento della consegna fino alla restituzione e/o revoca e dovrà porre ogni cura nella sua conservazione, per evitare danni, smarrimenti o sottrazioni.

Per il corretto uso del telefono l'assegnatario dovrà attenersi inoltre alle seguenti indicazioni:

1) la durata delle chiamate deve essere la più contenuta possibile in relazione alle esigenze di servizio;
2) qualora il dipendente si trovi presso gli uffici dell'Ente, è opportuno che utilizzi gli apparecchi di rete fissa per comunicare con altri dipendenti, utilizzando ove possibile la numerazione interna della linea VoIP;

Per il corretto uso del dispositivo USB per la connessione dati, l'assegnatario dovrà attenersi alle seguenti indicazioni:

3) il dispositivo dovrà essere utilizzato esclusivamente sui computer di proprietà dell'ente, in particolare sul portatile assegnato per il lavoro agile o da remoto;
4) qualora il dipendente si trovi presso gli uffici dell'Ente è opportuno che utilizzi il collegamento via cavo o WI-FI per l'accesso alla rete aziendale;
5) al termine del tempo di lavoro dovrà essere effettuata una disconnessione dalla rete mobile.

Per il corretto uso del portatile l'assegnatario dovrà attenersi inoltre alle seguenti indicazioni:

6) Il computer dovrà essere utilizzato esclusivamente con le proprie credenziali del dominio AIT.

Per tutti gli apparati:

7) operare nel rispetto delle disposizioni normative generali, evitando attività che producano deliberatamente spreco di risorse, danni o comunicazione - diffusione di dati, violazione della riservatezza ed altri usi impropri, quali l'introduzione o la diffusione di c.d. virus informatici;
8) in caso di furto, danneggiamento o smarrimento dell'apparato, l'assegnatario dovrà darne immediata comunicazione scritta al proprio Dirigente di Area/Responsabile diretto ed al Responsabile del Servizio Gestione Patrimonio ed Acquisti;
9) in caso di furto, danneggiamento o smarrimento della SIM, l'assegnatario dovrà darne immediata comunicazione scritta al proprio Dirigente di Area/Responsabile diretto ed al Responsabile del Servizio Gestione Patrimonio ed Acquisti, al fine di provvedere al blocco della stessa.

   Nel caso in cui il furto o lo smarrimento si verifichino in circostanze in cui non è possibile comunicare tempestivamente con il Dirigente di Area/Responsabile di servizio e con il Responsabile del Servizio Gestione Patrimonio ed Acquisti, l'assegnatario dovrà provvedere personalmente al blocco della SIM coinvolta contattando il gestore di telefonia mobile.
   L'assegnatario dovrà successivamente presentare la formale denuncia alla Polizia Giudiziaria di furto o smarrimento e farne pervenire copia al Dirigente di

Area/Responsabile diretto ed al Responsabile del Servizio Gestione Patrimonio ed Acquisti tramite il protocollo dell'Ente.
In caso di malfunzionamento o di guasto dell'apparecchio o della SIM l'assegnatario dovrà prendere contatti con l'Ufficio Acquisti e Gestione Patrimonio:

· Dr.ssa Daniela Dragoni tel. 055/26329404 – d.dragoni@autoritaidrica.toscana.it

L'Amministrazione declina ogni responsabilità per contravvenzioni o sinistri imputabili all'uso del telefono cellulare durante la guida di autoveicoli o altro utilizzo improprio.

Con l'occasione, si riportano le 11 raccomandazioni pubblicate da AgID il 17 marzo 2020, per uno Smart working sicuro:

- Segui prioritariamente le policy e le raccomandazioni dettate dalla tua Amministrazione;
- Utilizza i sistemi operativi per i quali attualmente è garantito il supporto;
- Effettua costantemente gli aggiornamenti di sicurezza del tuo sistema operativo;
- Assicurati che i software di protezione del tuo sistema operativo (Firewall, Antivirus, ecc) siano abilitati e costantemente aggiornati;
- Assicurati che gli accessi al sistema operativo siano protetti da una password sicura e comunque conforme alle password policy emanate dalla tua Amministrazione;
- Non installare software proveniente da fonti/repository non ufficiali;
- Blocca l'accesso al sistema e/o configura la modalità di blocco automatico quando ti allontani dalla postazione di lavoro;
- Non cliccare su link o allegati contenuti in e-mail sospette;
- Utilizza l'accesso a connessioni Wi-Fi adeguatamente protette
- Collegati a dispositivi mobili (pen-drive, hdd-esterno, etc) di cui conosci la provenienza (nuovi, già utilizzati, forniti dalla tua Amministrazione)
- Effettua sempre il log-out dai servizi/portali utilizzati dopo che hai concluso la tua sessione lavorativa.

OBBLIGHI DI RISERVATEZZA E PROTEZIONE DEI DATI

Ciascun lavoratore dovrà svolgere la prestazione con la diligenza richiesta dalla natura della prestazione stessa, garantire la riservatezza delle informazioni e dei dati, utilizzando all'uopo particolari accortezze, legate alla peculiarità delle modalità di svolgimento del proprio lavoro. Dovrà, dunque, rispettare l'obbligo della riservatezza, di non diffusione delle informazioni, del segreto d'ufficio, nonché ogni altro obbligo espressamente previsto nel contratto di lavoro, nell'atto di nomina a responsabile e/o autorizzato al trattamento dei dati (atti che qui si intendono integralmente richiamati).
Il lavoratore dovrà, inoltre, conservare e custodire diligentemente e responsabilmente le informazioni (personali e non), afferenti all'attività lavorativa, su supporto cartaceo o digitale, impegnandosi, fra le altre, a non renderle visibili e/o accessibili a soggetti terzi non autorizzati.
Il lavoratore ha l'obbligo, infine, di comunicare immediatamente al datore di lavoro ogni violazione o sospetto di violazione dei dati personali che dovesse riguardare informazioni di titolarità dell'Ente, trattate nell'espletamento della prestazione lavorativa.

In particolare, con riferimento alle modalità smart work, si richiama l'attenzione sui seguenti

punti:

- porre ogni cura per evitare che ai dati possano accedere persone non autorizzate presenti nel luogo di prestazione lavorativi fuori sede;
- procedere a bloccare l'elaboratore in dotazione in caso di allontanamento dalla postazione di lavoro, anche per un intervallo molto limitato di tempo;
- alla conclusione della prestazione lavorativa giornaliera è obbligatorio conservare e tutelare i documenti eventualmente stampati provvedendo alla loro eventuale distruzione solo una volta rientrato presso l'abituale sede di lavoro;
- qualora, invece, in via d'eccezione, al termine del lavoro risulti necessario trattenere presso il domicilio materiale cartaceo contenente dati personali, lo stesso dovrà essere riposto in armadi, cassetti o altri contenitori muniti di serratura.

RESPONSABILITA' e RUOLI

Ciascun lavoratore risponderà nei confronti di terzi di ogni eventuale trattamento illecito dei dati, personali e non, manlevando l'Ente da ogni responsabilità al riguardo.

L'Ente, nel rispetto della normativa in materia di protezione dei dati personali, di cui al Regolamento UE 2016/679 e del Codice privacy, rimarrà Titolare del trattamento dei dati.

Il lavoratore, ancorché la prestazione è svolta nella forma del lavoro agile o da remoto, rimarrà autorizzato al trattamento; dovrà, pertanto, attenersi scrupolosamente agli obblighi e a tutto quanto stabilito nel relativo atto di autorizzazione.

In alcun modo il Titolare potrà avere accesso a file o a informazioni personali contenute all'interno del dispositivo che non siano inerenti all'attività lavorativa.