Allegato B)

DISCIPLINARE RELATIVO ALL'UTILIZZO DELLE STRUMENTAZIONI INFORMATICHE DA PARTE DELLO SMART WORKER

Sommario

TITOLO I - DISPOSIZIONI GENERALI

Art. 1 - Oggetto - Ambito di applicazione

1. Il presente documento individua le specifiche tecniche minime di custodia e sicurezza dei dispositivi elettronici e dei software, nonché le regole necessarie a garantire la protezione dei dati e delle informazioni del Comune di ____. In particolare, disciplina le modalità di accesso ed utilizzo degli strumenti informatici, di internet, della posta elettronica, messi a disposizione dall'Amministrazione ai suoi dipendenti nell'ambito della modalità di lavoro agile (in seguito anche smart working) sia nel caso in cui sia stato concesso l'uso di risorse informatiche di proprietà dell'Amministrazione sia nel caso il dipendente usi la propria strumentazione informatica.

2. Le risorse infrastrutturali sono costituite dalle componenti hardware e software.

3. Il patrimonio informativo è l'insieme delle banche dati in formato digitale ed in generale di tutti i documenti prodotti tramite l'utilizzo delle risorse infrastrutturali.

Art. 2 - Principi generali

Ogni utente è responsabile, civilmente e penalmente, del corretto uso delle risorse informatiche, con particolare riferimento ai servizi, ai programmi cui ha accesso e ai dati trattati a fini istituzionali.

È altresì responsabile del contenuto delle comunicazioni effettuate e ricevute a fini istituzionali anche per quanto attiene la riservatezza dei dati ivi contenuti, la cui diffusione impropria potrebbe configurare violazione del segreto d'ufficio o della normativa per la tutela dei dati personali. Sono vietati comportamenti che possono creare un danno, anche di immagine, all'Amministrazione.

Nell'esecuzione della prestazione lavorativa in modalità agile, il dipendente è tenuto al rispetto degli obblighi di riservatezza, ai sensi del "Regolamento recante codice di comportamento dei dipendenti pubblici" e del codice di condotta approvato dall'Amministrazione.

La struttura competente in materia di sistemi informativi (in seguito anche "Servizio CED") supporta il servizio di assistenza agli utenti (in seguito anche smart workers), avvalendosi di personale specializzato, sia esso personale dipendente dell'Amministrazione stessa, che personale esterno in outsourcing.

Art. 3 - Modalità di accesso ai servizi informatici dell'Amministrazione.

1. Il dipendente in modalità di lavoro agile accede ai servizi informatici resi disponibili dall'Amministrazione. Di regola utilizzando le credenziali di accesso già possedute per ragioni d'ufficio.

2. Per l'utilizzo dei servizi di cui al comma 1 il dipendente accede mediante VPN SSL (Virtual Private Network) e un sistema di autenticazione username/password.

3. Il dipendente agile, dopo il collegamento alla VPN dell'Amministrazione e tramite le credenziali di cui al comma 2 dell'articolo 3, si connette attraverso la VPN alla propria postazione di lavoro abituale sulla quale dispone dei servizi applicativi utili allo svolgimento dell'attività lavorativa in coerenza con l'accordo individuale di lavoro stipulato con l'Amministrazione.

5 Il personale sistemistico e tecnico-informatico del Servizio CED, incaricato della gestione e della manutenzione dei componenti del sistema informatico, possono accedere alle postazioni di lavoro anche con strumenti di supporto/assistenza e diagnostica remota, per effettuare interventi di manutenzione preventiva e correttiva, richiesti dall'utente, oppure in caso di oggettiva necessità, a seguito di rilevazione di problemi tecnici sulla postazione. Gli operatori di norma non accedono ai dati di lavoro, a meno che l'intervento richiesto non sia focalizzato su questi ultimi, e comunque esclusivamente alle componenti hardware/software strettamente necessarie alla risoluzione della problematica e sono tenuti rigorosamente al rispetto del segreto d'ufficio e delle norme vigenti sulla privacy.

6. Ogni dipendente che, per qualsiasi motivo, lasci incustodita la propria postazione di lavoro è tenuto a bloccare l'accesso al computer portatile stesso o spegnere fisicamente l'apparato in questione.

TITOLO II - UTILIZZO DELLA STRUMENTAZIONE DELL'ENTE

Art. 5 - Dotazioni informatiche ai dipendenti nell'ambito della modalità di lavoro agile

1. La dotazione informatica eventualmente assegnata al dipendente in modalità di lavoro agile è specificata nell'accordo individuale.

2. Gli strumenti informatici messi a disposizione del lavoratore agile (ad esempio, computer portatile, accessori, software, ecc.) sono di proprietà dell'Amministrazione. Il lavoratore deve custodire ed utilizzare gli strumenti informatici, i dispositivi di accesso a internet, la posta elettronica e i servizi informatici e telematici in modo appropriato e diligente ed è responsabile della propria postazione di lavoro.

Art. 6 - Modalità di utilizzo degli strumenti informatici

1. Il computer portatile eventualmente affidato allo smart worker è uno strumento di lavoro. Ogni utilizzo improprio, non inerente all'attività lavorativa può contribuire a creare disservizi anche agli altri utenti, nonché minacce alla sicurezza informatica.

2. Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale del Servizio CED del Comune né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti.

3. Non è consentito disinstallare o inabilitare il programma antivirus e antimalware installato dal Servizio CED. Ogni eventuale malfunzionamento di quest'ultimo va segnalato tempestivamente alla predetta struttura competente in materia di sistemi informativi.

4. Non è consentito modificare la configurazione impostata sul proprio computer portatile, nonché installare periferiche (hard-disk, DVD, fotocamere, apparati multimediali, ecc ...) esterne agli strumenti in dotazione se non per esigenze di servizio, autorizzate dal Servizio CED che provvederà direttamente ad eseguire queste operazioni.

5. Non è consentita la consultazione, memorizzazione e diffusione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

6. È consentita esclusivamente l'installazione di supporti per la connessione mobile per l'accesso a Internet messi a disposizione dall'Amministrazione o da essa autorizzati. Qualunque esigenza in tal senso deve essere comunicata al Servizio CED, che ha il compito di analizzare la problematica per addivenire ad una soluzione coerente con le vigenti politiche di sicurezza ed integrità della rete.

7. L'eventuale malfunzionamento o danneggiamento degli strumenti informatici deve essere tempestivamente comunicato ai Sistemi Informativi.

TITOLO III - UTILIZZO DISPOSITIVI PERSONALI

Art. 7 - Installazione app per ricevere le telefonate dal proprio interno

L'autorizzazione allo svolgimento di attività in smart working è condizionata alla disponibilità del dipendente ad installare sul cellulare di servizio, o sul proprio cellulare se sprovvisto di cellulare di servizio, l'APP specifica associata al centralino telefonico utilizzato dall'ente che consente di ricevere le telefonate indirizzate al proprio interno di lavoro direttamente sul dispositivo mobile.

Art. 8 – Salvataggio documenti.

E' fatto divieto al dipendente di salvare documenti d'ufficio sul proprio PC personale.

TITOLO IV - DISPOSIZIONI FINALI

Art. 9 – Richiamo ad altre disposizioni

Il dipendente in smart working è tenuto al rispetto del DISCIPLINARE RELATIVO ALL'UTILIZZO DEI DATI approvato con _____ e ss.mm.ii. nonché alle regole di comportamento indicate nella "Guida pratica al lavoro agile nella PA" scaricabile dal sito https://www.funzionepubblica.gov.it/

E' fatto obbligo al dipendente in smart working di chiudere la connessione VPN subito dopo aver concluso la sessione di lavoro.

Art. 10 – Integrazione codice di condotta

Le disposizioni di cui al presente documento integrano il codice di condotta dell'ente e ne rappresentano parte integrante.

Art. 11 - Controlli, responsabilità e sanzioni

1. Il computer portatile o altro apparato in dotazione al dipendente agile è configurato dall'Amministrazione in modo da consentirne l'utilizzo esclusivamente per finalità lavorative e per la salvaguardia della sicurezza e dell'integrità dei dati e dell'infrastruttura tecnologica.

2. L'Amministrazione si riserva di effettuare verifiche sul corretto utilizzo degli strumenti informatici, della posta elettronica, di Internet, nel rispetto delle normative vigenti e del presente documento.

3. Gli eventuali controlli, compiuti dal personale incaricato del Servizio CED, potranno avvenire mediante un sistema di controllo dei contenuti (utilizzo di Proxy server che creino "barriera di difesa" verso il web, agendo da filtro per le connessioni entranti ed uscenti e monitorando, controllando e modificando il traffico interno) o mediante “file di log” della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati non oltre tre mesi, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell’Ente.

5. La violazione da parte degli utenti dei principi e delle norme contenute nel presente documento comporta l'applicazione delle sanzioni previste dalle disposizioni contrattuali vigenti in materia, previo espletamento del procedimento disciplinare.

Art. 12 - Aggiornamenti delle regole tecniche

1. Le disposizioni generali contenute nel presente documento possono essere soggette ad aggiornamenti, integrazioni e/o correzioni, in relazione all'evolversi della tecnologia, all'entrata in vigore di sopravvenute disposizioni di legge o all'evolversi delle esigenze dell’Amministrazione.