COMUNE DI SAN STINO DI LIVENZA

Città Metropolitana di Venezia

DISCIPLINARE PER IL CORRETTO USO DEGLI STRUMENTI INFORMATICI PER IL DIPENDENTE IN LAVORO AGILE

Revisione	Data emissione	Motivo della revisione	Visto preparazione	Visto approvazione	Estremi di approvazione
01	21/10/2022	Prima emissione	Responsabile CED	Segretario Generale	-

1 Premesse e scopo del documento

Il Comune di San Stino di Livenza intende con il presente atto, individuare e indicare ai propri dipendenti alcune istruzioni aggiuntive per il corretto trattamento dei dati personali nell'ambito dello svolgimento delle mansioni lavorative sotto forma di lavoro agile.

I dipendenti del Comune (in seguito anche Amministrazione) nell'ambito della modalità di lavoro in mobilità a cui sia stato concesso l'uso di risorse informatiche di proprietà dell'Amministrazione ovvero in caso di utilizzo di risorse informatiche di proprietà del lavoratore medesimo (in seguito anche utente) devono rispettare le specifiche tecniche minime di custodia e sicurezza dei dispositivi elettronici e dei software, nonché le regole necessarie a garantire la protezione dei dati personali e delle informazioni afferenti l'Amministrazione.

Il presente regolamento costituisce una integrazione del Regolamento per la Protezione dell'Informazione adottato dal Comune di San Stino di Livenza con delibera di Giunta Comunale n. _ _ del 27/10/2022, per quanto concerne il corretto uso degli strumenti informatici per il lavoratore in situazione di lavoro agile.

1.1 Contesto Normativo

Questo documento fa riferimento al seguente quadro normativo:

- "*Regolamento (Ue) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*", che sarà direttamente applicabile in tutti gli Stati dell'Unione europea a partire dal 25 maggio 2018 (d'ora in poi "**GDPR**");

- D.lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali"(d'ora in poi "**Codice Privacy**") integrato con le modifiche introdotte dal *D.lgs. 10 agosto 2018, n. 101, Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE(regolamento generale sulla protezione dei dati).*

- Provvedimenti del Garante per la protezione dei dati personali in materia di "misure di sicurezza", in particolare con riguardo agli Amministratori di Sistema (Provvedimento generale del 27 novembre 2008).

- Garante della privacy "Linee guida per posta elettronica e internet" del 01.03.2007 pubblicato in Gazzetta Ufficiale n. 5 del 10 marzo 2007.

- Direttiva n. 2/2009 del Dipartimento Funzione Pubblica ad oggetto "Utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro".

- Legge 20 maggio 1970, n. 300 "*Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento*" (Statuto dei Lavoratori); Modificata dall'articolo 23 D.lgs. 14 settembre 2015 n. 151 (così detto *"Decreto sulle semplificazioni"* attuativo della Legge delega 10.12.2014 n. 183, anche nota come *"legge di riforma del diritto del lavoro"* o *"Jobs Act"*).

- Legge 7 agosto 2015, n. 124, art.14 recante *l'obbligo, per le amministrazioni pubbliche, di adottare, nei limiti delle risorse di bilancio disponibili a legislazione vigente e senza nuovi o maggiori oneri per la finanza pubblica, misure organizzative volte a fissare obiettivi annuali per l'attuazione del telelavoro* e successive modifiche apportate dal decreto-legge 2 marzo 2020, n. 9 recante *"Misure urgenti di sostegno per famiglie, lavoratori e imprese connesse all'emergenza epidemiologica da COVID-19"*, a mezzo delle quali viene *superato il regime sperimentale dell'obbligo, per le amministrazioni, di adottare misure organizzative per il ricorso a nuove modalità spazio-temporali per lo svolgimento delle prestazioni lavorative, con la conseguenza che la misura opera a regime*.

- Legge n. 81 del 2017 recante "*Misure per la tutela del lavoro autonomo non imprenditoriale e misure volte a favorire l'articolazione nei tempi e nei luoghi di lavoro subordinato*", art.18 comma 3 che prevede che le disposizioni introdotte in materia di lavoro agile si applicano, in quanto compatibili, anche ai rapporti di lavoro alle dipendenze delle amministrazioni pubbliche di cui all'art. 1, comma 2 del decreto legislativo 30 marzo 2001, n. 165.

- Direttiva n. 3 del 2017 della Conferenza unificata "*Linee guida contenenti regole inerenti all'organizzazione del lavoro finalizzate a promuovere la conciliazione dei tempi di vita e di lavoro dei dipendenti*", che definisce gli indirizzi per l'attuazione delle misure e linee guida contenenti le indicazioni metodologiche per l'attivazione del lavoro agile.

- Direttiva n. 1 del 25.02.2020: "*Prime indicazioni in materia di contenimento e gestione dell'emergenza epidemiologia da COVID-19 nelle pubbliche amministrazioni al di fuori delle aree di cui all'art. 1 del decreto-legge n. 6 del 2020*", ove le amministrazioni di indirizzo, nell'esercizio dei poteri datoriali, sono invitate a potenziare il ricorso al lavoro agile, individuando modalità semplificate e temporanee di accesso alla misura con riferimento al personale complessivamente inteso, senza distinzione di categoria di inquadramento e tipologia di rapporto di lavoro.

- Circolare n. 1/2020 del 04.03.2020 della Presidenza del Consiglio dei Ministri, Ministro per la Pubblica Amministrazione, recante "*Misure incentivanti per il ricorso a modalità flessibili di svolgimento della*

prestazione lavorativa" che prevede misure di incentivazione per le pubbliche amministrazioni, al fine di favorire l'utilizzo di modalità flessibili di svolgimento a distanza delle prestazioni lavorative.

1.2 Ambito di applicazione

Il presente documento si applica ad Amministratori e dipendenti, nell'ambito della modalità di lavoro agile.

2 Patrimonio Informativo e strumenti informatici

Il Regolamento per la Protezione dell'Informazione adottato dal Comune di San Stino di Livenza definisce come patrimonio informativo: *il complesso dei beni informatici siano essi banche dati memorizzate in database, aree documentali digitalizzate (documenti di vario tipo pdf, testi, fogli di calcolo…), archivi cartacei che in egual misura trattano dati personali, o anche non personali, che possono essere di natura riservata o non riservata e che costituiscono per l'appunto il complesso dei beni conoscitivi in possesso dell'Ente.*

Gli strumenti informatici sono costituiti dall'insieme delle risorse informatiche dell'Amministrazione e dalle risorse infrastrutturali e dal patrimonio informativo digitale (dati). L'Amministrazione promuove ogni opportuna misura organizzativa e tecnologica, volta a prevenire il rischio di utilizzi impropri delle strumentazioni e delle banche dati di proprietà dell'Amministrazione anche nell'ambito dello svolgimento dell'attività di lavoro in mobilità.

Ogni utente è responsabile 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.

Gli strumenti informatici utilizzati dal lavoratore in mobilità (ad esempio, computer portatile, accessori, software, ecc.) possono essere di proprietà dell'Amministrazione o del lavoratore. In ogni caso, il lavoratore deve custodire ed utilizzare gli strumenti informatici, Internet, la posta elettronica e i servizi informatici e telematici in modo appropriato e diligente ed è responsabile dell'uso strumentazione utilizzata per lo svolgimento della propria mansione.

Al dipendente in modalità di lavoro in mobilità sono attribuite le credenziali di autenticazione per l'accesso ai servizi informatici dell'Amministrazione. Di regola le credenziali in questione sono quelle già possedute dal dipendente per ragioni d'ufficio.

Il dipendente accede ai servizi informatici resi disponibili dall'Amministrazione mediante VPN SSL (Virtual Private Network).

Il dipendente medesimo, dopo il collegamento alla VPN dell'Amministrazione e tramite le credenziali ricevute, utilizza una propria postazione di lavoro.

L'Amministrazione rende disponibile sulla postazione di lavoro in mobilità gli strumenti software necessari per l'utilizzo dei servizi applicativi in un contesto di sicurezza e omogeneizzazione delle stesse postazioni di lavoro.

La postazione di lavoro dotate dall'Amministrazione per il lavoro in mobilità può essere utilizzata anche durante l'espletamento dell'attività lavorativa presso l'ordinaria sede di servizio.

Il computer portatile o eventualmente altro device mobile utilizzato al lavoratore, proprio o fornito dall'Ente, 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 ed espone a responsabilità, civile e penale, l'utente.

In caso di cessazione del rapporto di lavoro sarà cura dell'utente rimuovere ogni dato personale eventualmente presente sulle macchine in dotazione, prima che l'account individuale del dipendente venga disattivato.

Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico dell'Amministrazione mediante virus, malware o mediante ogni altro software aggressivo, quali l'apertura di messaggi di posta elettronica e dei relativi allegati di provenienza sospetta o non conosciuta e affidabile; la navigazione su siti web per ragioni non riconducibili all'attività lavorativa e così via.

Ogni utente è tenuto a controllare la presenza e il regolare funzionamento del software antivirus e antimalware eventualmente installato sul proprio computer portatile.

Nel caso che il software antivirus e antimalware rilevi la presenza di un virus e/o di un malware che non è riuscito ad eliminare, l'utente dovrà immediatamente sospendere ogni elaborazione in corso e spegnere il computer portatile e segnalare tempestivamente l'accaduto al Responsabile CED.

Sulle postazioni di lavoro in dotazione al dipendente in mobilità l'Amministrazione esegue scansioni pianificate allo scopo di verificare l'eventuale presenza di codici maligni.

3 Uso di periferiche e cartelle condivise

Per cartella condivisa (o "area di lavoro condivisa" o "condivisione") si intende uno spazio disco disponibile sui server centrali, per la memorizzazione di dati e programmi accessibili ad un gruppo di utenti preventivamente autorizzati.

L'utente è tenuto ad utilizzare le unità di rete per la condivisione di informazioni strettamente professionali; non può pertanto collocare, anche temporaneamente, in queste aree qualsiasi file che non sia attinente allo svolgimento dell'attività lavorativa. L'utente è tenuto, altresì alla periodica revisione dei dati presenti in tutti gli spazi assegnati, con cancellazione dei files che non necessitano di archiviazione e che non siano più necessari ai fini procedimentali.

Particolare attenzione deve essere prestata alla duplicazione dei dati al fine di evitare, salvo casi eccezionali, un'archiviazione superflua.

L'utilizzo delle periferiche condivise è riservato esclusivamente ai compiti di natura strettamente istituzionale, come tutti gli spazi di archiviazione messi a disposizione degli utenti da parte delle strutture Informatiche dell'Amministrazione.

Le credenziali (nome utente e password) per l'accesso ai servizi informatici vengono assegnate dal Responsabile CED, previa richiesta del Responsabile del servizio, nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente. Il Responsabile CED provvede inoltre a rigenerare password scadute o dimenticate ed a disattivare le utenze cessate (pensionamento, dimissioni ecc.) o a sospenderle in particolari casi.

L'utente deve essere consapevole del fatto che cedere le proprie credenziali, ovvero permettere a terzi l'accesso ai servizi comunali, significa autorizzarli a proprio nome alla gestione degli stessi, con effetti potenzialmente gravissimi (ad es. visualizzazione di informazioni riservate, alterazione o distruzione di dati, uso della propria posta elettronica etc.).

4 Dispositivi di archiviazione e salvaguardia dei dati

Fatte salve le politiche di salvataggio centralizzato dei dati conservati sui sistemi informatici e sulle postazioni di lavoro in mobilità, è consentito, previa autorizzazione da parte del Responsabile CED, l'eventuale uso di dispositivi di backup via USB (chiavette, hard disk esterni, etc.) in casi straordinari, purché i dati in essi contenuti siano comunque trattati ai sensi della normativa vigente in materia di dati personali, sensibili o giudiziari, e non vengano in nessun modo ceduti a terzi, se non nel perimetro della normativa citata e del trattamento necessario ai fini procedimentali.

La fornitura e l'uso di tali dispositivi di archiviazione USB dovranno essere concordati con il Responsabile CED, il quale dovrà provvedere ad una prima analisi e formattazione del contenuto esistente, al fine di ridurre le minacce informatiche.
Ogni utente è responsabile della custodia dei dati di lavoro presenti sulla propria postazione di lavoro informatica. Gli utenti hanno cura di conservare copia della documentazione di lavoro nelle aree condivise predisposte con il supporto del Responsabile CED.

5 Uso di internet

Il Regolamento per la Protezione dell'Informazione adottato dal Comune di San Stino di Livenza riporta: *L'Ente mette a disposizione dei propri utenti la possibilità di accedere alle proprie risorse informatiche anche dall'esterno dei confini dell'Organizzazione stessa, mediante per esempio rete VPN SSL (Virtual Private Network), un canale privato e criptato verso la rete interna. L'accesso mediante VPN/RDP viene concesso a consulenti, professionisti, tecnici e fornitori che nell'ambito di un rapporto contrattuale con l'Ente necessitino di accedere a determinate risorse informatiche. Viene concesso, altresì, a dipendenti e funzionari dell'Ente che necessitino di svolgere compiti specifici o siano in modalità di lavoro subordinato o smart working, pur non essendo presenti in sede.*
Le richieste di abilitazione all'accesso mediante tali canali di comunicazione dovranno essere autorizzate dal Responsabile CED o l'Amministratore di sistema suo sostituto. Qualora sia necessario l'accesso alla rete dell'Ente attraverso i suddetti strumenti e tecniche di collegamento è necessario prestare la massima attenzione nelle fasi di accesso, proteggendo da occhi o da telecamere presenti la fase di digitazione dell'utente e della password. Una volta aperta la connessione, questa deve rimanere attiva lo stretto necessario all'espletamento delle attività richieste, quindi chiusa. In ogni caso, prima di abbandonare la postazione dalla quale è stata aperta la connessione è bene accertarsi dell'avvenuta chiusura della stessa, eliminando cronologia e file temporanei (ove possibile) ed eventuali altri dati di connessione che l'amministratore di rete potrà indicare all'utente in fase di consegna delle credenziali di accesso..

Data la specificità della connessione VPN SSL, la navigazione Internet in modalità agile, viene disciplinata dalle stesse policy che garantiscono in modo efficiente la sicurezza delle postazioni all'interno dell'ente, verso le quali l'utente da remoto si collega.

La navigazione Internet dalla postazione remota di proprietà dell'utente, al di fuori della connessione VPN SLL, non può essere filtrata, per cui sarà cura dell'utente, al fine di evitare compromissioni di sicurezza:

- evitare la navigazione su categorie di siti potenzialmente illegali secondo normativa vigente (quali pedofilia, gioco d'azzardo, ecc.) o comunque ledenti la dignità umana (violenza, razzismo)
- evitare lo scambio di materiale protetto dalla normativa vigente in tema di tutela del diritto d'autore e utilizzare sistemi di scambio dati/informazioni con tecnologie "peer to peer" (dall'interno della rete all'esterno e viceversa) o sistemi di Anonymous Proxy.

Il PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento dell'Istituzione utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi proibita la navigazione in Internet per motivi diversi da quelli legati all'attività lavorativa. Ciascun dipendente /collaboratore si deve attenere alle seguenti regole di utilizzo della rete Internet e dei relativi servizi.
Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, l'Ente adotta uno specifico sistema di blocco o filtro automatico che prevengano determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una "black list". L'Ente si attiverà nell'individuazione di categorie di siti considerati correlati con la prestazione lavorativa. Gli eventuali controlli, compiuti dal personale incaricato dell'Ufficio CED, potranno avvenire mediante un sistema di controllo dei contenuti (Web Filtering) 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 30 giorni, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'Ente.

5.1 Posta Elettronica

Per quanto concerne l'uso della posta elettronica, valgono le disposizioni contenute nel Regolamento per la Protezione dell'Informazione, in particolare si ricorda:

La casella di posta elettronica assegnata all'utente è uno strumento di lavoro. Gli Utenti assegnatari delle caselle di Posta Elettronica sono responsabili del corretto utilizzo delle stesse e sono tenuti, in un'ottica di correttezza ed uso Responsabile degli strumenti, a contribuire alla riduzione del fenomeno dello "spam" (trasmissione su larga scala e in grandi volumi di e-mail non sollecitati). La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti per evitare che raggiunga dimensione eccessive.

Se l'e-mail ricevuta è destinata ad altre persone è necessario limitare il più possibile la lettura del documento, ovvero facendolo con il solo obiettivo di comprendere che non si tratta di documentazione propria (quindi senza né leggere il contenuto, né cercare di capire a chi appartiene), ma inviare un messaggio al mittente spiegando l'errore. L'e-mail ricevuta va immediatamente eliminata, anche dal cestino.

Per quanto riguarda la posta di interesse dell'Ente che erroneamente è pervenuta all'indirizzo individuale, va comunicato al mittente che ha spedito la posta di interesse dell'Ente all'indirizzo personale, che il recapito corretto è quello istituzionale dell'ente.

Nel caso vi fosse incertezza in ordine alla credibilità del messaggio e/o alla sua provenienza il dipendente dovrà contattare immediatamente Il Responsabile CED o l'Amministratore di sistema suo sostituto, o il personale preposto, per una valutazione del singolo caso.

Nel caso in cui fosse necessario inviare a destinatari esterni messaggi contenenti allegati con dati personali o dati personali sensibili, è obbligatorio che questi allegati vengano preventivamente resi inintelligibili attraverso

crittazione con apposito software (archiviazione e compressione con password). La password di crittazione deve essere comunicata al destinatario attraverso un canale diverso dalla e-mail (ad esempio per lettera o per telefono) e mai assieme ai dati criptati. Tutte le informazioni dell'Ente, i dati personali e/o sensibili di competenza dell'Ente possono essere inviati soltanto a destinatari - persone o Enti – qualificati e competenti

Le informazioni eventualmente raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 679/16 "General Data Protection".

6 Controlli, responsabilità e sanzioni

Il computer portatile o altro apparato in dotazione al dipendente in mobilità 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.
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.