Città metropolitana
di Venezia

ISTRUZIONI PER L'UTILIZZO DELLE RISORSE INFORMATICHE E PER IL TRATTAMENTO DEI DATI

Città metropolitana di Venezia

Art. 1 – Oggetto

Le presenti istruzioni disciplinano le condizioni per il corretto utilizzo degli strumenti informatici (postazioni desktop o portatili, nonché dispositivi "smartphone"), della rete, l'uso della posta elettronica e la navigazione in internet.

Viene definita la configurazione hardware e software delle Postazioni di Lavoro (PdL) assegnate agli utenti; ogni variazione rispetto a quanto previsto deve essere richiesta e motivata esclusivamente dal dirigente del Servizio ed autorizzata dal Servizio Informatica.

Vengono, altresì, definite le modalità di svolgimento dell'attività lavorativa in modalità agile (c.d. "Smart Working").

Art. 2 – Modalità di utilizzo dei dispositivi informatici

Nel seguito vengono descritte le modalità di utilizzo dei dispositivi informatici assegnati in custodia agli utenti.

Art. 2.1 – Modalità di utilizzo dei personal computer (Portatili o Desktop)

2.1.1 – L'accesso all'elaboratore è protetto da password per la cui disciplina si rimanda all'articolo 4 delle presenti istruzioni.

2.1.2 – La configurazione iniziale di ogni Personal Computer predisposta dal personale informatico non deve essere modificata.

2.1.3 – Non è consentito installare autonomamente programmi di qualunque tipo, se non previa richiesta del Dirigente del Servizio e verifica ed autorizzazione del Servizio Informatica. L'installazione sarà comunque effettuata dal personale informatico addetto su indicazione del responsabile della gestione e della manutenzione degli strumenti elettronici. È sempre vietato l'utilizzo di software "portable" installati su dispositivi di archiviazione mobile (es. chiavetta USB).

2.1.4 – È onere del Dirigente del Servizio verificare il coerente utilizzo delle risorse assegnate ed evitarne l'uso improprio o l'accesso da parte di personale non autorizzato, compreso l'utilizzo da parte di terzi in luoghi non presidiati.

2.1.5 – Il Personal Computer non deve mai risultare in stato di "sbloccato" quando non presidiato. In caso di temporanee assenze dall'ufficio, l'elaboratore, se non viene spento, deve essere lasciato

disconnesso oppure deve essere attivato lo screen saver con password abilitata ovvero bloccato sulla schermata di blocco.

2.1.6 – Non è consentito collegare direttamente sul proprio PC o mediante rete LAN nessun dispositivo di comunicazione o altro (modem, PC portatili ed apparati in genere), se non previa autorizzazione da parte del Servizio Informatica su richiesta motivata dal proprio Dirigente.

2.1.7 – Per quanto riguarda il trattamento dei dati personali "particolari", in base alle indicazioni del Dirigente responsabile del Servizio, vengono individuati dei profili di autorizzazione per ciascun utente incaricato o per classi omogenee di utenti incaricati, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento (principi di segregazione e minimizzazione). Periodicamente, e comunque almeno annualmente, verrà verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione, secondo quanto previsto dalla normativa vigente ed in particolare dal Regolamento UE 2016/679 in seguito GDPR, il D.Lgs 2003/196 e il D.Lgs 2018/101.

2.1.8 – Ai fini della protezione dei dati personali contenuti nelle postazioni, è vietato l'utilizzo da parte dell'utente di supporti di memorizzazione rimovibili quali – a titolo di esempio non esaustivo – CD, chiavette USB, hard disk esterni, ecc.
Qualora vi siano particolari esigenze che richiedano l'utilizzo di questi dispositivi, il Servizio Informatica può eccezionalmente autorizzarne l'impiego, a seguito di formale richiesta motivata dal Dirigente del Servizio. Gli utilizzatori dovranno adoperarsi, assumendosene la responsabilità, per la corretta custodia dei supporti al fine di escludere accessi non autorizzati agli stessi ed ai dati in essi contenuti provvedendo, ad esempio, all'attivazione della crittografia (se possibile) e, comunque, riponendoli in appositi armadi/cassetti chiusi a chiave: i dispositivi prima di essere utilizzati, dovranno essere preventivamente verificati tramite il software antivirus in dotazione.

2.1.9 – Non sono consentite la compilazione, ricerca, diffusione e memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica salvo che questi non siano necessari per la propria attività lavorativa.

2.1.10 – L'utente è responsabile della postazione di lavoro assegnatagli (Computer, Monitor, mouse, lettori smart card, stampanti locali, etc.), deve custodirla con la massima diligenza e restituire i dispositivi consegnati.

2.1.11 – Il disco locale del PC così come i supporti removibili eccezionalmente autorizzati ed assegnati, non sono oggetto delle procedure di salvataggio dati e pertanto l'utente dovrà farsi carico di eseguirle in

autonomia ed eventualmente chiedendo supporto al servizio informatica.

2.1.12 – Qualora l'utente utilizzi il disco locale del PC o supporti removibili eccezionalmente autorizzati ed assegnati, dovrà prestare attenzione al trattamento degli stessi ai sensi della normativa sulla privacy (con particolare riferimento al GDPR, il D.Lgs 2003/196 e il D.Lgs 2018/101).

2.1.13 – Nel caso di trasferimenti di ufficio degli utenti la postazione di lavoro (PC e tutte le attrezzature informatiche in dotazione all'utente trasferito) verrà trasferita nel nuovo ufficio di assegnazione e verranno riconfigurate le policy di accesso alle risorse di rete secondo le indicazioni del funzionario e del dirigente di riferimento. Solamente nel caso in cui la posizione vacante venga ricoperta la postazione di lavoro rimarrà a disposizione dell'ufficio di riferimento. Qualora la postazione rimanga inutilizzata il Servizio Informatica procederà al recupero dei materiali e alla loro ricollocazione presso altri uffici.

2.1.14 – Al fine di garantire un corretto funzionamento delle postazioni di lavoro e di individuare eventuali software non autorizzati, i tecnici preposti all'amministrazione dei sistemi (utilizzando un apposito software di inventariazione) producono periodici report (ogni 3 mesi) in formato elettronico nei quali vengono evidenziati i software installati nei PC della rete.

Art. 2.2 – Modalità di utilizzo dei dispositivi smartphone

2.2.1 – Ad alcuni dipendenti, in funzione dei loro incarichi ed incombenze, può venir assegnato (su richiesta motivata del Dirigente del Servizio) un dispositivo di telefonia mobile (smartphone).

2.2.2 – Il servizio economato è l'ufficio competente per la gestione e l'assegnazione degli apparati mobili: al momento della consegna ogni dipendente autorizzato ha sottoscritto un modulo "Informativa per l'erogazione del servizio…" nel quale viene normato l'utilizzo dell'apparato telefonico e gli obblighi per il personale dipendente. L'informativa è reperibile nella Intranet al percorso "Settori→Economato→Avvisi".

2.2.3 – L'utilizzo dei dispositivi mobili è inoltre regolamentato dal "Regolamento per l'assegnazione e l'utilizzo delle apparecchiature di telefonia mobile" approvato con delibera di Giunta provinciale n. 84 del 7/3/2006, scaricabile dal sito della città metropolitana https://www.cittametropolitana.ve.it alla sezione "Disposizione Generali→Atti Generali".

2.2.4 – Per ragioni di sicurezza e di protezione dei dati è necessario proteggere lo smartphone di servizio con:

- PIN della SIM attivato al fine di impedire un utilizzo non autorizzato della SIM associata ad un'utenza della Città Metropolitana di Venezia;
- PIN del telefono (o altro sistema di blocco analogo eventualmente biometrico) al fine di impedire l'utilizzo dello smartphone da parte di persone diverse dall'assegnatario;
- Contenuto delle notifiche su schermata di blocco nascosto al fine di impedire letture accidentali dalla schermata di blocco da parte di soggetti diversi dall'assegnatario.

Inoltre è necessario effettuare l'installazione delle sole applicazioni scaricabili esclusivamente dallo store ufficiale (PlayStore per dispositivi Android oppure AppStore per dispositivi iOS) e strettamente legate alla propria attività lavorativa.

Qualora venga autorizzata l'utilizzo di una scheda SD (secondo le modalità previste dal punto 2.1.8 secondo capoverso) quale estensione di memoria del dispositivo, dovrà essere attivata la funzionalità di crittografia del supporto di memoria al fine di impedirne l'uso senza conoscere il PIN di sblocco.

2.2.6 – In caso di furto o smarrimento del dispositivo si configura un'ipotesi di "data breach" ai sensi dell'art. 4 comma 12 del GDPR. In questo caso, oltre a quanto previsto dal "Regolamento per l'assegnazione e l'utilizzo delle apparecchiature di telefonia mobile", l'utente assegnatario dovrà dare comunicazione immediata del furto/smarrimento o, comunque, entro 24 ore dalla conoscenza dell'accadimento, alla Città metropolitana di Venezia all'indirizzo gdpr@cittametropolitana.ve.it , specificando se le misure di sicurezza di cui al punto 2.2.4 erano attive ovvero disattivate, ciò ai fini dell'effettuazione della notifica al Garante della Privacy che dovrà avvenire a cura dell'Ente entro 72 ore dalla conoscenza del fatto, ai sensi dell'art. 33 del GDPR. L'utente dovrà, altresì, sporgere denuncia di furto/smarrimento alle autorità competenti (carabinieri o polizia).

Art. 3 – Utilizzo della rete della Città Metropolitana di Venezia

3.1 – Le cartelle di rete che contengono i dati dei servizi dell'Ente devono essere esclusivamente impiegate da parte degli utenti e ciascuno è responsabile del loro corretto utilizzo. Non ne è consentito l'uso da parte di persone non autorizzate. Per richiedere l'accesso alla rete informatica è necessario compilare il modulo "*ALLEGATO 1: Richiesta di accesso alla rete informatica*"

3.2 – L'accesso alle aree di rete da parte degli utenti, viene regolamentato dai tecnici preposti all'amministrazione dei sistemi tramite dei profili di accesso concordati con i Responsabili dei Servizi; tali profili di accesso e le politiche di accesso alle aree di rete, vengono verificati con cadenza annuale o su

specifica richiesta del Responsabile del Servizio interessato.

3.3 – Le unità di memorizzazione di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Su queste unità, i tecnici preposti all'amministrazione dei sistemi svolgono regolari attività di controllo, amministrazione e backup.

3.4 – I tecnici preposti all'amministrazione dei sistemi possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la sicurezza sia sulle unità di rete sia sui PC degli utenti.

3.5 – Costituisce buona regola di gestione delle unità di memorizzazione di rete da parte degli utenti, la periodica (almeno ogni tre mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, al fine di agevolare le copie di sicurezza e i salvataggi di backup.

3.6 – Non è consentito collegare qualsiasi dispositivo, diverso da quelli assegnati, alla rete dell'Ente (inclusa la rete Wireless).

3.7 – Non è consentito all'utente modificare le caratteristiche impostate sui PC forniti, i punti rete di accesso e le configurazioni delle reti LAN/WAN presenti nelle sedi.

3.8 – I tecnici preposti all'amministrazione dei sistemi, previa autorizzazione dell'utente (che può presidiare l'operazione), possono accedere attraverso un programma di controllo remoto ad ogni PC per interventi di assistenza e/o manutenzione.

3.9 – Ad ogni utente è assegnata un'area di rete ad accesso esclusivo (solitamente indicata come disco U) nelle risorse del computer all'interno della quale l'utente può archiviare dati che siano relativi alla propria attività o vita lavorativa (es. cedolini, report timbrature, ecc.).

3.10 – L' "albero di rete" (disco Y), è formato in modo che in radice vi sono tante aree quante sono le sedi più importanti della Città Metropolitana di Venezia. All'interno di ogni area/sede sono contenute le aree di rete dei settori/servizi. All'interno di ogni "sede" è presente un'area denominata "SCAMBIO" che funge da base di appoggio per lo scambio di dati tra gli utenti dei diversi settori dell'Ente. I dati contenuti nelle aree "SCAMBIO" vengono cancellati settimanalmente il sabato.

3.11 – Al fine di preservare le aree di rete, i tecnici preposti all'amministrazione dei sistemi eseguono periodiche (ogni 3 mesi) scansioni dei dati con il fine di individuare e rimuovere eventuali file o archivi non pertinenti con le attività professionali e provvederanno a comunicarne la natura e la titolarità dei files, al Responsabile del Servizio competente sull'area di rete interessata.

3.12 – Alla cessazione del servizio di un dipendente, l'account di accesso alla rete verrà chiuso e la sua posta elettronica verrà cancellata come indicato all'articolo 8.9. Per solerzia nei confronti dell'utenza, il dipendente, prima di cessare il servizio, può richiedere, per un periodo non superiore alle due settimane oltre la data di chiusura della collaborazione, l'attivazione di un risponditore automatico con un messaggio da concordare nel quale notificare la conclusione del rapporto di lavoro con Città metropolitana di Venezia (*vedi ALLEGATO 4 - RICHIESTA DI ATTIVAZIONE MESSAGGIO RISPONDITORE AUTOMATICO DI POSTA PER CESSAZIONE DAL SERVIZIO*).
Trascorsi i termini, gli account di posta e di rete verranno immediatamente e definitivamente chiusi; verrà inoltre ritirata la dotazione informatica in carico all'utente per essere assegnata ad altro utilizzo.

3.13 – In alcune zone delle sedi principali della Città Metropolitana di Venezia è presente una rete WiFi (WiFI_PVE) che consente ai dispositivi portatili forniti dall'Ente ed opportunamente configurati dal Servizio Informatica, di accedere alle risorse della rete come se fossero connessi via cavo; tale rete WiFi è protetta ed è ad uso esclusivo dei dispositivi forniti dall'Ente.
È presente inoltre una rete WiFi (WiFi_PVE_GUEST) ad accesso libero nella quale gli utenti e gli ospiti possono connettersi utilizzando delle opportune credenziali richieste al Servizio Informatica: la richiesta avviene tramite un form che compare automaticamente sul browser del dispositivo che richiede l'accesso dopo che è stata fatta la connessione alla rete WiFi. Il traffico telematico può essere sottoposto, a fini di sicurezza, a politiche di data retention ai sensi della normativa vigente con particolare riferimento a quanto previsto dal GDPR, dal D.Lgs 2003/196 e dal D.Lgs 2018/101.

3.14 - È severamente vietato utilizzare le risorse della Citta Metropolitana di Venezia per i seguenti scopi :

- Violare la sicurezza delle risorse di rete, tra cui, ma non solo, l'accesso ai dati, server o account ai quali non si e autorizzati; aggirare l'autenticazione utente su qualunque dispositivo; sniffing del traffico di rete.
- Causare l'interruzione di servizi della Citta Metropolitana di Venezia o di altre risorse di rete, tra cui, ma non solo, provocare inondazioni ICMP, fare packet spoofing, denial of service, heap overflow, o acquisire informazioni di routing forgiato per scopi dannosi.
- Introdurre honeypot, honeynets, creare nodi TOR o tecnologie simili sulla rete della Citta Metropolitana di Venezia.
- Utilizzare qualunque software di anonimizzazione della connessione, compresa la configurazione di servizi VPN o l'utilizzo della rete TOR.

- Utilizzare tecniche di SQL-Injection, XSS, CSRF o qualsiasi altro attacco web-based con lo scopo di effettuare attività di privilage escalation su server/client sia collegati alla rete della Città Metropolitana di Venezia sia all'esterno della stessa.
- Violare la legge sul copyright, compresi, ma non limitatamente, la duplicazione illegale o la trasmissione di immagini protette da copyright, musica, video e software.
- Esportare o importare software, informazioni tecniche, software di crittografia, o tecnologia in violazione delle leggi internazionali o regionali.
- Utilizzare Internet o la rete della Citta Metropolitana di Venezia in violazione della normativa corrente.
- Accedere a siti pornografici o pedopornografici.
- Introdurre intenzionalmente codice malevolo incluso, ma non solo, viruses, worms, Trojan horses, e-mail bombs, spyware, adware e keyloggers.
- Utilizzare software di crittografia per cifrare contenuti che violino i punti precedenti.
- Port scanning di rete o scansioni di sicurezza sulla rete.

3.15 – Le attività dettagliate al punto 3.14 possono essere consentite qualora siano necessarie all'espletamento della propria attività lavorativa purché esse non costituiscano reato (es. è consentito effettuare SQL-Injection qualora la propria attività sia la creazione di un portale web del quale si vuole testare la sicurezza ma non può essere consentito effettuare la stessa attività su un sito esterno). Le eccezioni di cui al presente punto devono essere debitamente e formalmente autorizzate dal Servizio Informatica.

3.16 – L'utente che senza l'autorizzazione prevista dal punto 3.15 proceda all'esecuzione delle attività di cui al punto 3.14, si assume la piena responsabilità dell'atto e ne risponderà in prima persona qualora quanto compiuto costituisca reato e questo venga perseguito dalle autorità competenti.

Art. 4 – Gestione delle password

4.1 – La password è strettamente personale e deve essere custodita dall'utente con la massima diligenza e non divulgata. Le password di ingresso alla rete e di accesso ai programmi sono attribuite inizialmente dai tecnici preposti all'amministrazione dei sistemi. La password di rete deve essere modificata al primo accesso.

4.2 – Le password devono essere lunghe almeno 8 caratteri, salvo impedimenti tecnici delle applicazioni,

formate da lettere maiuscole e/o minuscole, numeri e caratteri speciali quali & % ^ # $ e non dovranno contenere parti dello username, ricordando che lettere maiuscole e minuscole hanno significati diversi per i sistemi, evitando ovviamente contenuti di senso logico immediato che sono facilmente individuabili o associabili all'utente (per es. nomi/date di nascita e simili).

4.3 – La password di rete utilizzata dagli utenti ha una durata massima di 3 mesi. Il cambio della password di accesso alla rete e di tutte le applicazioni integrate è imposto ogni tre mesi dal sistema di autenticazione tramite policy. L'utente viene avvisato all'avvicinarsi della scadenza attraverso notifiche del domain controller. La nuova password non potrà essere uguale alle 2 precedenti.
Le altre password devono essere diligentemente modificate dall'utente con cadenza trimestrale.

4.4 – Ogni password deve essere immediatamente sostituita, nel caso si sospetti che la stessa abbia perso la segretezza.

4.5 – Qualora l'utente venga a conoscenza delle password di altro utente, è tenuto a comunicarglielo immediatamente e, in caso di impossibilità, al suo dirigente che lo comunicherà ai tecnici preposti all'amministrazione dei sistemi per la disabilitazione delle credenziali compromesse.

4.6 – È obbligo dei Responsabili di Settore comunicare tempestivamente ai tecnici preposti all'amministrazione dei sistemi eventuali cambi di mansione dei dipendenti che comportino modifiche o revoche di autorizzazione all'accesso delle risorse informatiche.

4.7 – Qualora per motivi urgenti ed inderogabili di servizio, si rendesse necessario accedere al pc di un utente assente (compreso l'accesso alla sua casella di posta elettronica) con le sue credenziali, il dirigente del servizio chiederà ai tecnici preposti all'amministrazione dei sistemi di cambiarne la password. La nuova password verrà comunicata in maniera riservata al Dirigente del Servizio, il quale informerà l'utente al suo rientro. L'utente dovrà cambiare nuovamente la password di accesso al sistema secondo quanto previsto dal punto 4.1.

4.8 – Le password di accesso agli applicativi dell'ente o ai portali istituzionali devono essere conservate con la massima cura. Non possono essere salvati in rete o nel pc file in chiaro contenenti le password.

Art. 5 – Composizione della Postazione di Lavoro

5.1 – La postazione di lavoro è costituita da un personal computer (fisso o portatile), un monitor, una tastiera ed un mouse.

Art. 6 – Utilizzo Stampanti

6.1 – In generale la stampa di dati e documenti deve essere evitata in ogni situazione e si deve ricorrere a questa possibilità solo se il documento cartaceo è essenziale allo svolgimento della propria attività lavorativa. La valutazione di tale necessità è a cura dell'utente il quale, in caso di stampa, deve adoperarsi per ritirare i documenti dai vassoi delle stampanti nel più breve tempo possibile.

6.2 – Qualora la stampa contenga dati personali particolari è opportuno, se possibile, scegliere una stampante che consenta l'utilizzo della modalità "stampa privata" ed impostare un codice per evitare che i documenti prodotti rimangano visibili a persone non autorizzate al trattamento dei dati in essi contenuti.

6.3 – Non è consentito in nessun caso stampare documenti personali.

6.4 – L'utente è tenuto ad utilizzare le stampanti di rete ricordando che è opportuno evitare di stampare documenti o file molto lunghi o di contenuto grafico importante: per tali file è possibile usufruire dei servizi della Stamperia in gestione al Servizio Economato.

Art. 7 – Utilizzo di PC portatili e/o accessori temporaneamente assegnati

7.1 – L'utente è responsabile del PC portatile e/o accessori (alimentatore, webcam, mouse, borsa, etc…) temporaneamente assegnati dal Servizio Informatica, previa richiesta del Dirigente del Servizio e deve custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo fino alla loro riconsegna.

7.2 – Ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

7.3 – I PC portatili utilizzati all'esterno (convegni etc.), contenenti dati dell'Ente, devono essere custoditi in un luogo protetto.

7.4 – Eventuali configurazioni di tipo Accesso Remoto, mediante linea telefonica sono a cura dei tecnici preposti all'amministrazione dei sistemi. È vietato utilizzare le suddette connessioni all'interno delle sedi della Città Metropolitana se contemporaneamente connessi alla rete LAN per la potenziale pericolosità di una doppia apertura verso l'esterno.

7.5 – I beni strumentali temporaneamente assegnati devono essere riconsegnati nei tempi concordati.

7.6 – In caso di furto/smarrimento si applicano le disposizioni di cui al punto 2.2.6 fatti salvi i richiami al punto 2.2.5, sostituiti in questo contesto con la dichiarazione della presenza di una password di protezione dell'utente utilizzato nel PC portatile.

Art. 8 – Uso della posta elettronica

8.1 – Ad ogni dipendente della Città Metropolitana di Venezia viene assegnata una casella di posta elettronica del dominio @cittametropolitana.ve.it. Per utilizzare la casella di posta elettronica istituzionale è necessario compilare l'allegato "*ALLEGATO 1: RICHIESTA DI ACCESSO ALLA RETE INFORMATICA*"

8.2 – Per ogni gruppo di lavoro e servizio sono assegnati normalmente indirizzi di posta elettronica di gruppo (liste di distribuzione) che consentono di ricevere o di inviare email collettivamente ai componenti del gruppo individuato.

8.3 – La posta elettronica, quale strumento di lavoro, deve essere consultata e manutenuta quotidianamente.

8.4 – Per la trasmissione di file all'interno della Città Metropolitana di Venezia è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati. Qualora la dimensione degli stessi superi 25 Megabyte, è opportuno utilizzare le aree di rete appositamente predisposte (Area di rete "SCAMBIO" di cui al punto 3.10, o eventuali servizi FTP/Cloud Drive messi a disposizione dal Servizio Informatica). Per motivi di sicurezza vengono bloccati dai sistemi antivirus i files suscettibili di contenere eseguibili pericolosi o script.

8.5 – È severamente vietato inviare catene telematiche (o di Sant'Antonio), messaggi di phishing, pubblicità, SPAM e simili.

8.6 – Si deve evitare l'invio di messaggi di posta elettronica contenenti dati personali comuni o particolari privilegiando altri strumenti che consentano una maggiore sicurezza.

8.7 – E' **consigliato** l'utilizzo della casella e-mail per i soli fini istituzionali. In particolare è vietato utilizzare la propria casella @cittametropolitana.ve.it per l'iscrizione a portali commerciali o a servizi online non attinenti la propria attività lavorativa.

8.8 – La casella di posta elettronica @cittametropolitana.ve.it è **suscettibile di accessi da parte dell'amministrazione** (esclusivamente secondo quanto previsto dall'art. 4.7) che quindi può venire a conoscenza del contenuto della corrispondenza.

8.9 – La casella di posta elettronica verrà disabilitata entro 24 ore dalla cessazione del servizio del dipendente al quale è stata assegnata e i contenuti cancellati salvo quanto previsto dall'art. 3.12.

Art. 9 – Intranet

Il portale Intranet è un portale web interno alla rete provinciale ed è organizzato in modo da essere utilizzato da tutti i dipendenti dell'Ente. Dal portale Intranet è possibile accedere ai software istituzionali e ai link dei principali portali informativi dell'Ente. Il portale intranet inoltre è utilizzato come bacheca elettronica per le comunicazioni interne ai dipendenti e per la diffusione di informazioni e documenti di interesse generale dell'ente.

Gli utenti sono tenuti a consultare il portale Intranet almeno una volta al giorno.

Art. 10 – Uso della rete Internet e dei relativi servizi

10.1 – Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. È proibito ogni accesso ad Internet effettuato per motivi diversi da quelli strettamente funzionali all'attività lavorativa stessa. In particolare sono severamente vietati gli accesi per l'effettuazione di transazioni bancarie, acquisto di biglietti (di viaggio o per spettacoli), partecipazione a discussioni (forum/chat), utilizzo di social network di qualsiasi tipo, acquisti on line, accesso a siti pornografici, accesso ed utilizzo di casinò online e utilizzo di piattaforme di gioco online. Opportune eccezioni possono essere autorizzate dal Servizio Informatica dietro richiesta motivata del Dirigente del Servizio. Per poter navigare in internet è necessario compilare il modulo "*ALLEGATO 2 DICHIARAZIONE DI ASSUNZIONE DI RESPONSABILITÀ PER L'ACCESSO A INTERNET DALLE POSTAZIONI AZIENDALI*"

10.2 – Ai fini del monitoraggio delle performance della rete, la navigazione in internet può formare oggetto di controllo, rispettando i principi di pertinenza e non eccedenza ed in ottemperanza della normativa vigente con particolare riferimento al GDPR, D.Lgs 2003/196 e D.Lgs 2018/101.

10.3 – L'accesso ad internet avviene attraverso l'utilizzo di uno specifico servizio in grado di inibire il collegamento ad alcune pagine in base al loro contenuto o categoria di appartenenza. È facoltà esclusiva dell'Amministrazione decidere quali categorie di siti o siti specifici sono oggetto di restrizione in quanto non di interesse per l'attività lavorativa dei dipendenti. Tale impostazione può essere variata senza preavviso. In caso uno specifico sito o categoria di siti sottoposti a restrizione sia di interesse lavorativo, il Dirigente del Servizio può richiederne lo sblocco con comunicazione motivata al Servizio Informatica.

10.3-bis – La modifica delle impostazioni di connessione di accesso ad internet è severamente vietata. Opportune eccezioni possono essere autorizzate dal Servizio Informatica dietro specifica richiesta motivata del Dirigente del Servizio o per motivi tecnici urgenti.

10.4 – Il traffico Web viene costantemente monitorato e l'accesso a siti viene tracciato tramite la generazione di report aggregati relativi agli accessi alla rete che verranno utilizzati qualora si caratterizzi uno scorretto utilizzo della rete o si manifesti un danno funzionale della stessa. Le politiche di data retention di tali report sono stabilite in funzione di quanto previsto dal GDPR, dal D.Lgs 2003/196 e s.m.i (art.132.). I log di accesso ad Internet vengono conservati per 12 mesi.

10.5 – E' vietato effettuare la navigazione in incognito, l'utilizzo di Browser per l'accesso al Deep e Dark Web (come, ad es. TOR) o l'attivazione di modalità di accesso alla rete pubblica che consentano di eludere i servizi centralizzati di accesso ad internet.

Art. 11 – Protezione antivirus

11.1 – Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico operato da virus o da ogni altro software aggressivo (c.d. malware).

11.2 - Ogni utente è tenuto a controllare il regolare funzionamento e l'aggiornamento periodico del software antivirus installato e mediante gli appositi strumenti disponibili sul desktop: qualora ciò non accadesse l'utente deve avvisare i tecnici preposti all'amministrazione dei sistemi.

11.3 – Nell'utilizzo della posta elettronica ogni utente è tenuto a prestare la massima attenzione nell'aprire allegati o seguire le istruzioni che potrebbero portare all'esposizione delle credenziali di accesso alla rete dell'Ente (phishing).

11.4 – Oltre a quanto previsto dal punto 11.3 l'utente è tenuto a comunicare al personale del Servizio Informatica la ricezione di qualunque messaggio di posta elettronica sospetto.

11.5 – Qualora l'utente si renda conto di aver aperto un allegato sospetto oppure di aver seguito un link potenzialmente rischioso, dovrà darne tempestiva comunicazione al Servizio Informatica e seguire scrupolosamente le indicazioni di quest'ultimo (comprese le indicazioni di intervento "fisico" sul computer come, ad esempio, lo scollegamento del dispositivo dalla rete elettrica o dalla rete dati).

Art. 12 – Linee Guida per le attività di Smart working

12.1 –L'utente che per motivate ragioni deve usufruire dei servizi dell'ente in modalità Smart working o di connessione al Sistema Informativo della Città metropolitana di Venezia dall'esterno, può farne richiesta al servizio informatica, tramite il proprio Dirigente, utilizzando il modulo (*ALLEGATO 3*

MODULO DI RICHIESTA DI CONNESSIONE AL SISTEMA INFORMATIVO DELLA CITTA' METROPOLITANA DI VENEZIA) al Servizio Informatica

12.2 – La Città Metropolitana di Venezia mette a disposizione dei propri lavoratori i seguenti servizi fruibili direttamente da rete Internet. Si sottolinea che le credenziali di accesso sono le medesime utilizzate durante il lavoro in sede:

a) *Sistema di posta elettronica Microsoft Exchange*, accessibile all'indirizzo https://cmvemail.cittametropolitana.ve.it/owa. L'accesso si effettua utilizzando le stesse credenziali di accesso usate nelle postazioni personali dell'ufficio

b) Portale *SIAM* accessibile all'indirizzo: http://siam.cittametropolitana.ve.it/siam

c) Portale *Trasporti Eccezionali* accessibile all'indirizzo: https://trasportiec.cittametropolitana.ve.it/

d) Portale *6Sport* accessibile all'indirizzo: https://6sport.cittametropolitana.ve.it

e) Portale *Gare e Gestione Appalti* accessibile all'indirizzo: https://cmvenezia.pro-q.it/

f) Programma *Sviluppo e Gestione Informative GDPR* accessibile all'indirizzo: https://www.privacylab.it/IT/44/LOGIN-PRIVACYLAB/?goTo=1&logout=1

12.2-bis – Qualora tali servizi risultino insufficienti al normale svolgimento delle funzioni aziendali, l'Amministrazione può mettere a disposizione una modalità di collegamento di tipo Remote Desktop (o equivalente). Con tali modalità l'utente potrà collegarsi al proprio PC di ufficio operando come se fosse davanti allo stesso: il monitor della postazione in sede risulterà disattivato in modalità CTRL-ALT-CANC e non sarà possibile visualizzare l'attività dell'utente. Ulteriori indicazioni operative saranno comunicate al lavoratore autorizzato.

12.2-ter – Le modalità di connessione individuate al punto 12.2-bis possono essere modificate dal Servizio Informatica per motivazioni legate alle esigenze sia lavorative sia della tutela della sicurezza del sistema informativo.

12.3 – L'utente autorizzato può accedere ai servizi di Smart working attraverso l'accesso ad internet della propria abitazione, oppure attraverso un dispositivo mobile personale purché sia adeguata e sufficientemente stabile o in alternativa tramite dispositivo mobile aziendale. L'accesso potrà avvenire tramite il proprio pc personale, se espressamente specificato nel modulo di richiesta oppure tramite dispositivo fornito direttamente dall'amministrazione (*ALLEGATO 3 MODULO DI RICHIESTA DI*

CONNESSIONE AL SISTEMA INFORMATIVO DELLA CITTA' METROPOLITANA DI VENEZIA).

Inoltre, il dispositivo da cui si eseguono le attività di Smart working deve soddisfare i seguenti requisiti:

a) Uso di un sistema operativo per il quale il produttore garantisce supporto e aggiornamenti di sicurezza. Al momento della stesura delle presenti istruzioni i sistemi operativi rispondenti a questa caratteristica sono: Windows 10 oppure MacOS almeno versione 10.14 Mojave oppure Linux Ubuntu Desktop 20.04 o equivalente;

b) Aggiornamento del sistema operativo alle ultime patch di sicurezza;

c) Uso di un software antivirus aggiornato e se possibile di firewall configurato (anche di sistema);

d) Gli account utente usati per accedere al computer devono essere protetti da password personale;

e) L'account utilizzato dall'utente per le attività di Smart working, oltre a quanto previsto al punto d), deve essere strettamente personale e non condiviso con altri membri della famiglia, i quali non devono conoscere la password di accesso.

12.3-bis – Per prevenire possibili intercettazioni non intenzionali di dati, il collegamento internet utilizzato deve essere sicuro da potenziali accessi non autorizzati. La modalità di connessione preferita dovrebbe essere attraverso cavo ethernet e solo quando questa non è disponibile/possibile Wi-Fi. Nel caso di connessioni effettuate tramite rete Wi-Fi, la rete deve essere protetta con password (WPA2) sufficientemente sicura e il router che ne gestisce l'accesso deve essere accessibile soltanto a persone fidate: pertanto si sconsiglia la connessione tramite reti Wi-Fi pubbliche.

12.3-ter – Per minimizzare il rischio potenziale di danni ai dispositivi degli uffici, l'utente autorizzato che si avvale di strumenti propri per effettuare le attività di Smart working, almeno durante l'esercizio di tali attività, deve tenere i comportamenti descritti dall'Art. 11 anche nell'ambito delle attrezzature personali.

12.4 – È fatto divieto, durante il collegamento remoto al computer d'ufficio, di trasferire o copiare documenti, immagini e qualsiasi altro genere di files proveniente dalla memoria della postazione d'ufficio alla memoria del dispositivo usato per le attività di Smart working e viceversa.

12.5 – Al fine di garantire la riservatezza dei dati sui quali il dipendente autorizzato a svolgere l'attività lavorativa in modalità agile sta operando, è fatto obbligo di rispettare quanto previsto all'art. 2.1.5 del presente atto anche nell'utilizzo della strumentazione personale.

12.6 – Dal punto di vista operativo, inoltre, si raccomanda:

a) di comunicare tempestivamente i casi in cui si verifichi un incidente da cui potrebbe derivare una violazione di dati personali: a tal proposito si rammenta che l'Ente ha 72 ore di tempo dall'avvenuta conoscenza dell'accaduto per effettuare la notifica del "data breach" al Garante della privacy (art. 33 del GDPR);

b) di attuare ogni cautela a protezione del dispositivo utilizzato per lo Smart working soprattutto se viene trasportato;

c) di consultare frequentemente ed almeno quotidianamente la posta elettronica (accedendo al link dell'art. 12.2 punto a) oppure tramite l'applicazione di posta nel caso di collegamento remote desktop);

d) di svuotare la memoria degli appunti (il cosiddetto "copia-incolla") una volta terminato il servizio, effettuando un "copia-incolla" di testo inutile, per evitare di mantenere anche solo temporaneamente salvate password o dati particolari;

Art. 13 – Osservanza delle disposizioni in materia di Privacy

È obbligatorio per tutti i dipendenti attenersi alle disposizioni di legge in materia di privacy secondo quanto previsto dal GDPR, dal D.Lgs 2003/196 e dal D.Lgs. 2018/101 e s.m.i.

Art. 14 - Istruzioni generiche per il trattamento dei dati

In relazione al trattamento dei dati personali, il dipendente dovrà porre particolare attenzione rispetto a quanto previsto dal GDPR ed in particolare dovrà :

- procedere alla raccolta di dati personali, nelle modalità previste dalle sue mansioni e indicate in apposita informativa;
- consegnare agli interessati, al momento della raccolta dei dati, il modulo contenente l'informativa di cui agli artt. 13-14 del GDPR, salvo che l'informativa medesima sia stata fornita direttamente dal titolare o dal responsabile;

- raccogliere, sempre al momento della raccolta dei dati, il consenso espresso, documentato per iscritto, degli interessati ai trattamenti previsti, salvo che a ciò abbiano provveduto direttamente il Titolare o il Responsabile, e salvo i casi di esonero previsti dalla stessa legge;
- trattare i dati personali nella misura necessaria e sufficiente alle finalità proprie della banca dati nella quale vengono inseriti, secondo quanto espresso nell'informativa e, comunque, in modo lecito e secondo correttezza;
- adottare, nel trattamento dei dati, tutte le misure di sicurezza che siano indicate dal Titolare o dal Responsabile, in particolare dovrà:
    - per le banche dati informatiche, utilizzare sempre il proprio codice di accesso personale, evitando di operare su terminali altrui e/o di lasciare aperto il sistema operativo con la propria password inserita in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;
    - trattare i soli dati la cui conoscenza sia necessaria e sufficiente per lo svolgimento delle operazioni da effettuare rispettando strettamente il proprio profilo di autorizzazione;
    - conservare i supporti informatici e/o cartacei contenenti i dati personali in modo da evitare che detti documenti siano accessibili a persone non autorizzate al trattamento dei dati medesimi;
    - con specifico riferimento agli atti e documenti cartacei contenenti dati personali ed alle loro copie, restituire gli stessi al termine delle operazioni affidate;
    - utilizzare i supporti di memorizzazione usati solamente qualora i dati in essi precedentemente contenuti non siano in alcun modo recuperabili, altrimenti etichettarli e riporli negli appositi contenitori;
    - copie di dati personali su supporti rimuovibili sono permesse solo se parte del trattamento, copie di dati particolari devono essere espressamente autorizzate dal Responsabile del trattamento o dal Titolare. In ogni caso tali supporti devono avere un'etichetta che li identifichi e non devono mai essere lasciati incustoditi;
    - in caso si constati o si sospetti un incidente di sicurezza deve essere data immediata comunicazione al Responsabile del trattamento o al Titolare;

Art. 15 – Sanzioni

La violazione delle prescrizioni previste dalle presenti istruzioni, fatte salve ulteriori conseguenze di natura penale, civile e amministrativa, costituisce responsabilità disciplinare secondo quanto previsto dal Codice Disciplinare.

Venezia-Mestre, maggio 2022

Città metropolitana di Venezia

ALLEGATO 1: RICHIESTA DI ACCESSO ALLA RETE INFORMATICA

Richiesta di creazione e di uso di casella di posta elettronica per dipendenti/stagisti/collaboratori della Città metropolitana di Venezia[1]

Dichiarazione del Dirigente o Caposervizio

Il sottoscritto, Dirigente ovvero Caposervizio presso la Città metropolitana di Venezia, richiede:

1. che venga creato un profilo di accesso alla rete informatica
   - ☐ a partire dalla data ..... / ..... / ..... sino al giorno ..... / ..... / .....
   - ☐ ovvero a tempo indeterminato sino alla conclusione del rapporto di lavoro
2. che venga creata e resa attiva una casella di posta elettronica
   - ☐ a partire dalla data ..... / ..... / ..... sino al giorno ..... / ..... / .....
   - ☐ ovvero a tempo indeterminato sino alla conclusione del rapporto di lavoro

per l'utente .....,

C.F. ....., secondo quanto previsto e disposto dal "Regolamento per l'utilizzo delle risorse informatiche e di rete della Città metropolitana di Venezia".

Settore: .....

Sede: .....

Recapito telefonico: .....

email: .....@cittametropolitana.ve.it

Firma: ..... Data: .... / .... / .....

Riferimento ex art 14 GDPR per amministratore di sistema.

[1] Da scansionare e spedire via mail a: informatica@cittametropolitana.ve.it o far pervenire all'ufficio Informatica, Centro Servizi - Via Forte Marghera 191, Mestre.

Città metropolitana di Venezia

ALLEGATO 2 DICHIARAZIONE DI ASSUNZIONE DI RESPONSABILITÀ PER L'ACCESSO A INTERNET DALLE POSTAZIONI AZIENDALI[1]

Il sottoscritto, firmando il presente documento, riconosce di aver letto, compreso ed accettato integralmente le politiche e le regole della Città metropolitana di Venezia, riguardo l'utilizzo e l'accesso a Internet.

Il sottoscritto si assume inoltre la piena responsabilità in caso di violazione delle leggi e dei regolamenti riconducibili al suo accesso personale.

Nome e Cognome: .....

Codice fiscale: .....

Servizio/Settore: .....

Firma: .....

☐ acconsente al trattamento dei dati personali (Decreto legislativo 30 giugno 2003, n. 196)

☐ non acconsente al trattamento dei dati personali

(in caso di rifiuto al trattamento dei dati personali, il collegamento a Internet sarà disabilitato, con esclusione del sito aziendale, della posta elettronica, qualora necessaria, e dei siti istituzionali legati all'attività lavorativa).

Firma: ..... Data: ...../ ..... / .....

[1] Da scansionare e spedire via mail a: informatica@cittametropolitana.ve.it o far pervenire all'ufficio Informatica, Centro Servizi - Via Forte Marghera 191, Mestre.

Città metropolitana di Venezia

ALLEGATO 3 - MODULO DI RICHIESTA DI CONNESSIONE AL SISTEMA INFORMATIVO DELLA CITTA' METROPOLITANA DI VENEZIA

Alla dirigente del Servizio
Informatica

Oggetto: Autorizzazione dipendente alla connessione al Sistema Informativo della Città Metropolitana di Venezia da rete esterna.

Il/La sottoscritto/a ……, dirigente del Servizio/Settore ……autorizza il dipendente ……. (inquadrato nella categoria giuridica ……) alla connessione attraverso Remote Desktop Connection al proprio PC d'ufficio da rete esterna dal …/…/……. al …/…/……. per lo svolgimento delle seguenti attività: ……..…….

……..

Si comunica, inoltre, che la connessione richiesta è motivata dalle seguenti esigenze straordinarie:

……

……

Il sottoscritto dirigente, nel comprendere i rischi che la richiesta comporta, si assume la responsabilità nei casi di perdita e/o divulgazione di dati personali (data breach) che dovessero da essa derivare. Inoltre, il sottoscritto dirigente dichiara di aver correttamente informato il dipendente dei comportamenti corretti da tenere nel connettersi al proprio PC di ufficio da rete esterna; il dipendente, in tal senso, dichiara di aver compreso le indicazioni ricevute e si impegna, sotto la propria responsabilità, a rispettarle scrupolosamente.

Per effettuare la connessione (barrare la casella d'interesse):

- ☐ Si richiede fornitura di PC dell'Amministrazione da restituire al termine delle attività autorizzate;
- ☐ NON si richiede fornitura di PC dell'Amministrazione.(*)

La connessione viene autorizzata esclusivamente con modalità Remote Desktop così come configurata dal Servizio Informatica e, pertanto, con le misure di sicurezza da questo individuate come adeguate (come la crittografia del canale di connessione) al fine di proteggere il Sistema Informativo.

Data e Luogo: ……,

Il dipendente autorizzato — Il dirigente

Visto, si autorizza
Dott.ssa Franca Sallustio

(*) Per la connessione con strumentazione propria, il dipendente si impegna ad utilizzare dispositivi PC con sistema operativo aggiornato (Windows 10 oppure MacOS almeno versione 10.14 Mojave oppure Linux Ubuntu Desktop 20.04 o equivalente) e nei quali è installato un software antivirus aggiornato con frequenza almeno giornaliera

Città metropolitana di Venezia

ALLEGATO 4 - MODULO DI ATTIVAZIONE RISPONDITORE AUTOMATICO POSTA ELETTRONICA PER CESSAZIONE DAL SERVIZIO

Al Servizio Informatica

Oggetto: Richiesta attivazione risponditore automatico posta elettronica.

Il/La sottoscritto/a ……, che cesserà il servizio presso la Città metropolitana di Venezia il …/…/……., chiede l'attivazione del risponditore automatico di posta elettronica della casella ……..@cittametropolitana.ve.it per 2 settimane oltre la data di cessazione (Art 3.2 delle ISTRUZIONI PER L'UTILIZZO DELLE RISORSE INFORMATICHE) con il seguente messaggio: ……
……

……

……

……

Data e Luogo: ……, Il dipendente……

N.B.: il presente modulo deve essere inviato almeno 3 giorni prima della cessazione dal servizio all'indirizzo email: informatica@cittametropolitana.ve.it