COMUNE DI PORTO VIRO

REGOLAMENTO
PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI E TELEMATICI

Il presente regolamento disciplina le modalità di accesso e di uso della rete informatica e telematica del Comune di Porto Viro e dei servizi che, tramite la rete stessa, è possibile ricevere o offrire.

CAPO I - NORMATIVA DI RIFERIMENTO, PRINCIPI GENERALI, FINALITA' E AMBITO DI APPLICAZIONE

Art. 1 - Premessa

1. Le Informazioni sono un bene che ha un valore per l'Ente, e di conseguenza, necessitano di essere protette adeguatamente.
   Le informazioni possono essere presenti in molte forme: stampate o scritte su carta, memorizzate elettronicamente, trasmesse per posta o utilizzando altri mezzi telematici. Qualunque forma abbiano le informazioni o qualunque sia il mezzo su cui è condivisa o memorizzata un'Informazione, questa deve essere sottoposta ad adeguata protezione.
   La sicurezza delle informazioni è definita qui come il mantenimento della:
   a) **riservatezza**: l'assicurazione che le informazioni siano accessibili solo a coloro che sono autorizzati ad avere l'accesso;
   b) **integrità**: salvaguardare la precisione e la completezza dell'informazione e del metodo di elaborazione;
   c) **disponibilità**: l'assicurazione che gli utenti autorizzati abbiano accesso alle informazioni e ai beni quando richiesto.
   La sicurezza delle informazioni non può essere ottenuta affidando tale compito alla sola tecnologia (firewall, antivirus, ecc.), ma è ottenuta attraverso un approccio sistemico che consiste in criteri, pratiche, procedure, accorgimenti, e strutture organizzative.
2. Nel Comune DI Porto Viro è presente una struttura complessa definita ITC "Tecnologie dell'informazione e della comunicazione" Tale struttura è una risorsa dell'Ente per questo è importante riuscire a gestire in maniera rapida, efficace ed efficiente il volume crescente di informazioni. Proprio per questo motivo le I.C.T. vanno considerate come arma strategica in grado di mettere a disposizione dati e informazioni qualitativamente migliori nell'ambito dell'organizzazione e, grazie alla diffusione della tecnologia e dell'interconnettività, possono aiutare a ridefinire i propri rapporti interni ed esterni del Comune. Il fine ultimo delle tecnologie dell'informazione è il trattamento dei dati tramite conversione, immagazzinamento, protezione, trasmissione e recupero sicuro dei dati stessi.
3. La progressiva diffusione delle nuove tecnologie informatiche e, in particolare il libero accesso alla rete internet dai Personal Computer, espone il Comune ai rischi di un coinvolgimento sia patrimoniale che penale, creando problemi alla sicurezza e all'immagine dell'Ente stesso;
4. Le disposizioni emanate dall'Autorità Garante per la protezione dei Dati Personali con provvedimento n. 13 del 01/03/2007 (Allegato n. 1 al presente Regolamento) e la Direttiva n. 2 del 26.05.2009 emanata dal Ministero per la P.A. e l'Innovazione (Allegato n. 2 al presente Regolamento) in cui vengono definite le linee guida per l'utilizzo della posta elettronica ed internet sui luoghi di lavoro, impongono l'adozione di precise e definite regole per l'utilizzo di tali strumenti.

Art. 2 - Contesto Normativo

I principi applicati nella stesura del presente Regolamento sono tratti dal quadro normativo che segue:

- Art. 15 Costituzione;
- Norme del Codice Civile: artt. 2087, 2104, 2105 e 2106;
- L. 20 maggio 1970, n. 300 (Statuto dei lavoratori) artt. 4 e 8;

- D.Lgs 81 del 09/04/2008 e ss.mm.ii in materia di sicurezza sul lavoro con particolare riferimento all'allegato XXXIV, par. 3.
- Codice in materia di protezione dei dati personali (D. Lgs. n. 196/2003 e ss.mm.ii);
- Art. 49, D. Lgs 7 marzo 2005 n. 82, Codice dell'Amministrazione Digitale, "Segretezza della corrispondenza trasmessa per via Telematica" ss.mm.ii;
- "Linee guida del Garante per posta elettronica e internet", emanate con deliberazione 1° marzo 2007 n. 13;
- Direttiva n. 02/09, "Utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro" emanata dal Ministero per la Pubblica Amministrazione e l'Innovazione.
- Regolamento generale sulla protezione dei dati (GDPR, General Data Protection Regulation-Regolamento UE 2016/679)
- CIRCOLARE 17 marzo 2017, n. 1/2017: "Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015). (17A02399)"

Art. 3 - Finalità

1. Il presente regolamento è diretto a definire le modalità di accesso ed utilizzo degli strumenti informatici, della rete informatica e telematica e dei servizi che tramite la stessa rete è possibile ricevere all'interno e all'esterno dell'Amministrazione, ai fini di un corretto utilizzo degli strumenti stessi da parte dei dipendenti, degli amministratori e collaboratori del Comune di Porto Viro.
2. Nonostante l'utilizzo delle risorse informatiche e telematiche debba sempre ispirarsi al principio della diligenza e correttezza, principi di per sé contemplati nel codice di comportamento che regola l'agire dei dipendenti e dei collaboratori nell'ambito di un rapporto di lavoro, il Comune di Porto Viro adotta il presente Regolamento interno al fine di evitare che comportamenti inconsapevoli possano rappresentare un aumento del rischio per la sicurezza nel trattamento dei dati, ovvero che, comportamenti anche consapevoli, possano costituire infrazione al codice di comportamento dei dipendenti e dei collaboratori dell'Ente.
3. Il presente Regolamento disciplina le condizioni per il corretto utilizzo degli strumenti informatici da parte degli utenti con l'intento di:
   a) garantire la massima efficienza delle risorse informatiche e del loro utilizzo;
   d) garantire la riservatezza delle informazioni e dei dati;
   e) assicurare la continuità del servizio nell'interesse dell'Ente e dei Cittadini;
   b) garantire il rispetto delle leggi in materia di utilizzo delle risorse informatiche.

Art. 4 - Ambito di applicazione

1. La rete del Comune di Porto Viro è costituita dall'insieme delle risorse informatiche, cioè dalle risorse infrastrutturali e dal patrimonio informativo digitale.
   Le risorse infrastrutturali sono le componenti hardware/software e gli apparati elettronici collegati alla rete informatica comunale.
   Il patrimonio informativo è l'insieme delle banche dati in formato digitale ed in generale tutti i documenti prodotti tramite l'utilizzo dei suddetti apparati.
2. Il presente Regolamento si applica a tutti gli utenti interni che sono autorizzati ad accedere alla rete comunale. Per utenti interni si intendono i dipendenti a tempo indeterminato e determinato, senza distinzione di ruolo e di livello, nonché a tutti i collaboratori del Comune di Porto Viro a

prescindere dal rapporto contrattuale con lo stesso intrattenuto (collaboratori a progetto, staff, in stage ecc.), e tutti gli amministratori che abbiano accesso alla rete dell'Ente.

3. Il presente Regolamento viene portato a conoscenza di tutti i dipendenti e /o collaboratori per il tramite dei rispettivi Responsabili di settore/servizio.

Art. 5 - Principi generali

1. Il Comune di Porto Viro promuove l'utilizzo della Rete Informatica e Telematica, di Internet e della Posta Elettronica quali strumenti utili a perseguire con efficacia ed efficienza le proprie finalità istituzionali, in accordo con le linee guida e i principi delineati dalla normativa vigente.
   L'Amministrazione promuove altresì l'utilizzo della rete informatica quale strumento essenziale per migliorare la qualità dei servizi, per consentire la possibilità di erogazione di servizi on-line, la realizzazione di archivi elettronici sempre più completi e l'accesso ad informazioni ed atti che avvicinino sempre più l'Amministrazione ai Cittadini.
2. Gli strumenti informatici e telematici assegnati agli utenti sono strumenti di lavoro e, come tali, non devono essere usati per fini diversi dalla normale attività lavorativa.
   Ogni utente è responsabile, civilmente e penalmente, del corretto uso delle Risorse Informatiche, dei servizi/programmi a cui ha accesso e dei 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'Ente; gli utenti devono essere consapevoli delle potenzialità offerte dagli strumenti informatici-telematici, e devono impegnarsi ad agire con responsabilità e a non commettere abusi aderendo a un principio di autodisciplina

Art. 6 - Segreto d'ufficio e riservatezza dei dati

1. Il dipendente non può divulgare, pubblicare o comunicare in alcun modo a terzi, direttamente o indirettamente, in toto o in parte, le informazioni apprese in occasione dello svolgimento delle mansioni per le quali è stato assunto dall'Ente, né potrà usarle, sfruttarle o disporne in proprio o tramite terzi.

2. Gli obblighi del dipendente previsti in questo capo non termineranno all'atto di cessazione del rapporto di lavoro, se non in riferimento a quelle specifiche parti delle informazioni che il dipendente possa dimostrare che erano già di pubblico dominio al momento della conclusione del rapporto, o che lo sono diventate in seguito per fatto a lui non imputabile.

3. Premesso che per «Informazioni Riservate» si intendono tutte le informazioni di qualsivoglia natura riferite o apprese in occasione dello svolgimento di mansioni per le quali il soggetto è stato assunto dal comune, il dipendente si impegna a considerare le Informazioni Riservate come strettamente private e riservate e ad adottare tutte le misure necessarie per non pregiudicare la riservatezza di tali informazioni;

4. Il dipendente si impegna ad utilizzare le Informazioni Riservate unicamente allo scopo di effettuare lo svolgimento dell'attività cui è preposto e di conseguenza a non usare tali informazioni in alcun modo che arrechi danno al comune, né per alcun altro scopo di qualsiasi natura;

5. Gli impegni di cui al presente capo non proibiscono di comunicare Informazioni Riservate:

a. ad amministratori e dipendenti, anche di società direttamente controllate, avvocati, revisori, banche o altri consulenti ai quali la conoscenza di tali Informazioni è necessaria al fine dell'espletamento di attività funzionali al comune;

b. a soggetti diversi da quelli specificati alla precedente lettera a), qualora ciò sia stato autorizzato dal Titolare del trattamento;

6. L'obbligo di riservatezza non opera in caso di Informazioni Riservate:

   a. che al momento in cui vengono rese note siano di pubblico dominio;

   b. che diventino di pubblico dominio dopo essere state rese note per causa non imputabile al dipendente;

7. L'impegno di riservatezza di cui al presente capo si protrarrà anche dopo la cessazione del rapporto di lavoro e sino a quando le informazioni in oggetto non saranno rese di pubblico dominio.

CAPO II - CRITERI DI UTILIZZO DEGLI STRUMENTI INFORMATICI

Art. 7 - Modalità di accesso alla rete e agli applicativi: password ed account

1. L'utente che ottiene l'accesso alla rete e agli applicativi è tenuto ad osservare il presente regolamento e le altre norme disciplinanti le attività e i servizi che si svolgono via rete ed è tenuto a non commettere abusi e a non violare i diritti degli altri utenti e dei terzi.
2. L'utente che ottiene l'accesso alla rete e agli applicativi si assume la totale responsabilità delle attività svolte tramite la rete.
3. Qualsiasi accesso alla rete a agli applicativi viene associato ad una persona fisica cui imputare le attività svolte utilizzando il codice utente.
4. L'account è costituito da un codice identificativo personale (username o user id: cognome più iniziale del nome) e da una parola chiave (password scelta dall'utente).
5. Si distinguono password di accesso al personal computer, di accesso alla rete e di accesso ai programmi gestionali, ciascuno con una specifica parola chiave, in particolare:
   a. password di BIOS, per l'accesso al PC
   b. password di rete, per l'avvio e l'utilizzo del sistema operativo e di tutte le risorse di rete
   c. password per l'accesso a particolari programmi gestionali e applicativi.
6. Al primo collegamento alla rete e agli applicativi, l'utente deve modificare la password (parola chiave) comunicatagli dall'Amministratore di Sistema e deve rispettare le seguenti norme:
   - Al primo accesso la parola chiave ottenuta dal Custode delle password deve essere cambiata.
   - La parola chiave è segreta e non deve essere comunicata ad altri.
   - In nessun caso devono essere annotate password in chiaro sia su supporto cartaceo che informatico.
   - La parola chiave va custodita con diligenza e riservatezza, in quanto stabilisce un rapporto biunivoco, che permette di responsabilizzare l'incarico stesso.
   - La parola chiave deve essere costituita da una sequenza minima di otto caratteri alfanumerici e non deve essere facilmente individuabile, in particolare:
     ✓ Non deve contenere nomi comuni
     ✓ Non deve contenere nomi di persona

- ✓ Deve comprendere almeno 3 fra questi 4 set di caratteri:
  - -Lettere Maiuscole
  - -Lettere Minuscole
  - -Numeri
  - -Simboli (;,.:-!"£$%&='?^_+*)
- ✓ Deve essere diversa dallo User-Id
- ✓ Non deve essere riconducibile all'incaricato. Pertanto, la password non deve essere basata su informazioni personali, riferimenti familiari o comunque dati inerenti direttamente al soggetto titolare della password stessa.
- ✓ Non debbono essere utilizzate le configurazioni ed opzioni di "compilazione automatica" o ricorda password quando le credenziali di accesso sono utilizzate attraverso web browser (Gestionale, Posta Elettronica, ecc..).

- È necessario procedere alla modifica della parola chiave a cura dell'utente, incaricato al trattamento, oltre che al primo utilizzo, successivamente almeno ogni 3 mesi qualora non impostato dal sistema informatizzato. Il dipendente ha l'obbligo di non alterare la funzione "cambio password" che obbliga a modificare la password con cadenza trimestrale o semestrale (asseconda dei casi).;
- Qualora l'intestatario della password ritenga che un soggetto non autorizzato possa essere venuta a conoscenza della propria password dovrà provvedere immediatamente a cambiarla dandone comunque comunicazione al Titolare/responsabile del trattamento, come in caso di rivelazione volontaria per specifici motivi.

7. Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal personale preposto, previa formale richiesta del responsabile del Servizio nell'ambito del quale verrà inserito e andrà ad operare il nuovo utente. In tale circostanza sarà cura del Responsabile del Servizio indicare i privilegi di accesso ai vari applicativi per il nuovo utente. Lo stesso Responsabile di Servizio dovrà altresì comunicare al personale preposto l'eventuale cessazione del rapporto di lavoro con l'utente per la conseguente disattivazione dell'account;
8. In caso di assenze prolungate e programmate, qualora se ne ravvisi la necessità per espletare esigenze d'ufficio, il dipendente interessato può delegare in forma scritta un altro dipendente all'utilizzo del proprio personal computer, comunicandogli le password necessarie. L'utente che intenda avvalersi di tale delega deve darne comunicazione al personale preposto indicandone anche i tempi di attuazione e deve provvedere, al rientro in ufficio, alla sostituzione della password;
9. In assenza di tale delega l'Amministratore di Sistema, può accedere ai dati o alle applicazioni presenti su una risorsa informatica assegnata ad un utente in caso di prolungata assenza, irrintracciabilità o impedimento dello stesso utilizzando le credenziali di accesso di amministratore di rete o reinizializzando la relativa password dell'utente. Tale accesso deve essere esplicitamente richiesto in forma scritta e motivato dal Responsabile del Servizio cui l'utente appartiene e deve essere limitato al tempo strettamente necessario al compimento delle attività indifferibili per cui è stato richiesto. Dell'avvenuto accesso deve essere data comunicazione all'interessato al suo rientro il quale dovrà necessariamente procedere al cambiamento della password di accesso al sistema.
10. Per motivi di sicurezza e protezione dei dati, ogni attività compiuta nella Rete Informatica può essere sottoposta a registrazione in appositi file "log" e riconducibili ad un account di rete. Detti file 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. La riservatezza delle informazioni in essi contenute è soggetta a quanto dettato dal D.Lgs. n. 196/2003 e ss.mm.ii. ed il regolamento europeo sulla privacy 27 aprile 2016 n. 2016/679 - G.U.U.E. n. 119, 4 maggio 2016, Serie L.

Art. 8 - Utilizzo dei dispositivi informatici

1. I dispositivi informatici (personal computer, portatili, stampanti ecc.) sono strumenti di lavoro e il loro utilizzo deve essere finalizzato esclusivamente allo svolgimento delle attività professionali e istituzionali dell'Amministrazione.
   Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.
   La collocazione del personal computer nella propria postazione di lavoro deve essere tale da ridurre il rischio di utilizzo a fini impropri e non legati all'attività lavorativa.
2. Ogni utente deve tenere comportamenti corretti, tali da preservare il buon funzionamento degli strumenti e tali da ridurre i rischi per la sicurezza del sistema informatico, quali l'utilizzo di supporti per la memorizzazione dei dati non sicuri e CD/DVD/USB provenienti dall'esterno, al fine di non diffondere virus.
3. L'accesso all'elaboratore è protetto da password che deve essere custodita dall'utente con la massima diligenza e non divulgata. Ogni singola postazione non deve essere lasciata incustodita. È necessario spegnere o bloccare il personal computer (CTRL+ALT+CANC e poi blocca computer) al termine dell'attività lavorativa e in caso di assenza prolungata dal proprio ufficio: lasciare un elaboratore incustodito connesso alla rete può essere la causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne l'indebito uso.
4. le dotazioni informatiche vengono consegnate complete di quanto necessario per svolgere le proprie funzioni, pertanto è vietato modificarne la configurazione.
   - I software installati sono quelli richiesti dalle specifiche attività lavorative dell'operatore. *E' pertanto proibito installare autonomamente qualsiasi programma, senza l'autorizzazione* (in forma scritta tramite e-mail) del Responsabile incaricato. in quanto sussiste il grave pericolo di portare virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore stesso.
   - Il comune, peraltro, ricorda all'utilizzatore che costituiscono illecito penale le condotte consistenti nella illecita duplicazione o riproduzione di software ai sensi della legge sul diritto d'autore n. 633/41.
   - Non è consentito modificare le impostazioni del BIOS o modificare le configurazioni hardware e software predefinite dall'Amministratore di Sistema.
   - Non è consentito l'uso di programmi diversi da quelli autorizzati ed installati ufficialmente dal personale autorizzato del Comune di Porto Viro. L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software gestionale esistente, può esporre l'Ente a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato o comunque libero.
5 Le regole sulle impostazioni e configurazioni dei Personal Computer vengono fornite dal DPO (Data Protection Officer) attualmente nominato di concerto con il Titolare del Trattamento ed il personale incaricato all'attuazione di quanto indicato. Qual ora si rendessero necessarie modifiche alle configurazioni impostate sul PC in uso, occorre darne comunicazione al Titolare del Trattamento.
6 Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

7. È vietata l'installazione non autorizzata di dispositivi di memorizzazione, comunicazione o altro (come ad es. masterizzatori, dispositivi di memorizzazione USB, dispositivi wireless, smartphone ecc.) se non con l'autorizzazione (in forma scritta tramite e-mail) del personale preposto.
8. Non è consentito aprire canali informativi non autorizzati da e verso l'esterno all'Amministrazione Comunale in qualsiasi forma (trasferimento su USB, dischi esterni, via internet ecc.).
9. È vietata la connessione alla rete comunale di apparati atti ad effettuare connessioni non autorizzate con reti esterne (es. router, bridge, access point wireless etc.).
10. Il personale incaricato potrà procedere alla rimozione di ogni dispositivo e di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sui singoli personal computer segnalandolo al Titolare del Trattamento dei Dati. Inoltre, Il titolare del trattamento si riserva di eliminare qualsiasi elemento: hardware e software la cui installazione non sia stata appositamente prevista o autorizzata.
11. Qualsiasi file estraneo all'attività lavorativa o non espressamente autorizzato, non può, nemmeno in via transitoria, essere salvato sul pc in uso del dipendente.
12. L'Amministratore di Sistema potrà accedere ai dati e agli strumenti informatici esclusivamente per permettere all'Amministrazione, titolare del trattamento, di accedere ai dati trattati da ogni incaricato con le modalità fissate dallo stesso Ente, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività dell'Ente nei casi in cui si renda indispensabile ed indifferibile l'intervento, ad es. in caso di prolungata assenza od impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato. L'amministratore di sistema potrà, altresì, accedere ai personal computer (anche con strumenti di supporto, assistenza e diagnostica remota) per manutenzione preventiva e correttiva, previa autorizzazione dell'interessato.
13. Tutti i dati sensibili riprodotti su supporti informatici o su supporti cartacei devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato da terze parti estranee all'Ente.
14. Fermo restando il principio di responsabilità individuale di ciascun utente, è responsabilità del dirigente verificare il coerente utilizzo delle risorse assegnate ed evitarne l'uso improprio o l'accesso alle risorse da parte di personale non autorizzato.
15. In caso di furto hardware e software è onere dell'utente, o del responsabile del servizio di appartenenza, effettuare denuncia all'autorità di polizia e far pervenire all'Amministratore di Sistema copia della denuncia.
16. Data Breach: i dati personali conservati, trasmessi o trattati dall'ente possono essere soggetti al rischio di perdita, distruzione o diffusione indebita, ad esempio a seguito di attacchi informatici, accessi abusivi, eventi avversi, come incendi o altre calamità. Si tratta di situazioni che possono comportare pericoli significativi per la privacy degli interessati cui si riferiscono i dati.
17. Nel caso in cui l'operatore del Comune riscontri una violazione delle banche dati dell'ente contenenti dati personali ne deve dare immediata informazione al Titolare o al Responsabile incaricato.
18. Il titolare deve avviare una procedura di comunicazione all'autorità garante del trattamento dei dati come previsti all'articolo 33 e 34 del R- UE 679/2016.

Art. 9 - Utilizzo di personal computer portatili

1. L'utente è responsabile del computer portatile assegnatogli dall'*Amministratore di Sistema* e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
2. Ai computer portatili si applicano le stesse regole di utilizzo previste per i computer desktop connessi in rete.
3. I notebook utilizzati all'esterno devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari, per evitare danni o sottrazioni;
4. Tali disposizioni si applicano oltre che per i portatili anche per gli altri dispositivi (quali videoproiettori, macchine fotografiche, tablet ecc.) anche nei confronti di incaricati esterni in caso di affidamento temporaneo in occasione di convegni, mostre ecc.
5. Il dirigente vigila sul corretto utilizzo del personal computer portatile e ne è corresponsabile col lavoratore che deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
6. In caso di furto è onere dell'utente, o del responsabile del servizio di appartenenza, effettuare denuncia all'autorità di polizia e far pervenire all'Amministratore di Sistema copia della denuncia.

Art. 10 - Utilizzo delle stampanti, dei FAX e dei materiali di consumo

1. L'utilizzo delle stampanti e dei materiali di consumo in genere (carta, inchiostro, toner, supporti digitali) è riservato esclusivamente ai compiti di natura strettamente istituzionale. Devono essere evitati in ogni modo sprechi dei suddetti materiali o utilizzi eccessivi, privilegiando altresì soluzioni operative che mirino al risparmio, come ad esempio privilegiando la stampa fronte retro, nonché soluzioni operative che mirino ad evitare l'utilizzo di carta (memorizzazione di documenti scansionati e comunicazione via e-mail) nell'ottica delle direttive inerenti alla digitalizzazione della Pubblica Amministrazione.
2. È cura del personale effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti e fotocopiatori comuni (soprattutto per le stampanti di rete siti in luoghi facilmente accessibili al pubblico). È buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.
3. In caso di stampe molto lunghe scegliere la stampante più adatta onde evitare sprechi di toner o cartucce e, nel caso di stampanti che fungono anche da fotocopiatrici, pianificare, se possibile, la stampa in particolari momenti della giornata in modo da non interferire con la normale attività lavorativa;
4. Quando si aprono determinati sportelli delle stampanti, bisogna aver cura di chiuderli rispettando rigorosamente la posizione che avevano prima dell'apertura.
5. Nel momento in cui si inserisce la carta nei cassetti di alimentazione, evitare di inserire carta sgualcita, rovinata o umida.
6. Il cambio cartucce lo si fa se si è sicuri di poterlo fare senza causare danni all'apparecchiatura, in caso contrario contattare gli addetti al sistema informatico e/o la ditta del noleggio dei fotocopiatori.
7. Quando si cambiano le impostazioni di un fotocopiatore e/o stampante, alla fine del proprio lavoro, si deve obbligatoriamente ripristinare l'assetto originario.

8. Quando si finisce la carta nei fotocopiatori di rete, è buona norma ricaricare la macchina, in modo che i successivi fruitori la trovino pronta per l'utilizzo.
9. Ogni utente sarà dotato di una password per stampare presso i fotocopiatori multifunzione dipartimentali siti nei corridoi dell'Ente in ottemperanza a quanto disposto dal Regolamento 679/2016. In questo modo gli operatori saranno presenti all'uscita dei documenti stampati ed eviteranno in questo modo il furto di dati personali.
10. Si raccomanda di non lasciare documenti incustoditi presso le postazioni di fax all'atto dell'invio. Qualora il dipendente sia prossimo a ricevere atti contenenti dati o informazioni riservate via fax, avrà cura di monitorare la postazione fax e preservare – limitatamente alle oggettive possibilità – la conoscibilità di tali dati o informazioni, da parte di terzi non autorizzati.

Art. 11 - Utilizzo di dispositivi di memorizzazione esterni

1. L'utilizzo di pen-drive USB è da evitare in quanto fonte probabile di virus informatici; il mezzo consigliato per il trasferimento dei dati è la posta elettronica che automaticamente controlla i documenti allegati segnalando eventuali file dannosi. Qualora si dovesse comunque procedere all'uso delle pen-drive USB è necessario eseguire un controllo preventivo antivirus sui dati in esse contenute;
2. Quando presenti, tutti i supporti riutilizzabili (CD, DVD, dispositivi di memorizzazione USB, etc.) contenenti dati sensibili e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. I dati memorizzati si possono infatti recuperare anche dopo la loro cancellazione. In caso di dismissione, per evitare problemi di sicurezza, questi supporti dovranno essere adeguatamente smaltiti e distrutti.
3. I supporti come i CD o i DVD con contenuto non autoinstallante possono essere utilizzati liberamente. Diversamente, quando un CD o un DVD tenta di installare del software sulla macchina l'operazione deve essere interrotta immediatamente, in questo caso contattare il personale preposto per eventuali ragguagli. Anche se generalmente non è rischioso utilizzare il lettore ottico del PC in dotazione per riprodurre CD o DVD musicali o comunque multimediali, si ricorda che è illegale detenere file musicali e/o video protetti dai diritti d'autore, in formato compresso o non compresso (mp3, wav, wma, avi, mpeg, ecc.) ottenuti con metodi ritenuti illegali dalle norme sul diritto d'autore. Si invitano pertanto gli utenti che avessero memorizzato tali file nei PC del Comune di Porto Viro o che detenessero copie masterizzate non autorizzate di CD o DVD, di procedere alla cancellazione definitiva dei file e alla rimozione dei supporti contraffatti al fine di non incorrere nelle sanzioni previste dalla normativa vigente.
4. Sui PC dotati di scheda audio e/o di lettore CD non è consentito l'ascolto di programmi, files audio o musicali, se non a fini prettamente lavorativi.
5. È fatto obbligo conservare, custodire e controllare i supporti informatici removibili contenenti dati, informazioni, notizie o immagini di attinenza aziendale, affinché nessun soggetto terzo ne prenda visione o possesso.

CAPO III - CRITERI DI UTILIZZO DELLO STRUMENTO DI BACKUP

Art. 12 - Utilizzo del dispositivo di Backup

1. Dati e le informazioni gestite ed archiviate in modalità informatica costituiscono patrimonio dell'Ente finalizzato all'erogazione di servizi istituzionali. Di conseguenza, allo scopo di consentire la piena disponibilità di tale patrimonio, la gestione informatizzata dei dati, deve

privilegiare l'utilizzo di sistemi gestionali accentrati, indipendenti dalla singola postazione di lavoro, governati da livelli di autorizzazione predeterminati (user-id/password, ruolo/profilo). Per questo motivo è stato messo a disposizione da parte del personale preposto un'area Documentale di rete su apposito server.

2. Il documentale è composto da cartelle di rete su server a disposizione dei vari Settori ed Uffici. Ogni Settore ha uno spazio la cui dimensione è limitata e determinata in funzione delle esigenze del settore, della disponibilità dell'intero sistema di memorizzazione, del numero di utenti, dei volumi e tipologia di documenti trattati.
3. L'organizzazione e la gestione dell'albero delle sottocartelle sarà programmata tramite policy concordata con il responsabile del Settore/Servizio stesso.
4. Le cartelle di rete sono periodicamente salvate con cadenza minima di un giorno ed i corrispondenti salvataggi sono disponibili per un arco temporale massimo di 30 giorni.
5. Le cartelle di rete sono aree di condivisione di documenti strettamente istituzionali e non possono, in alcun modo, essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia correlato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità
6. Ogni utente è responsabile dei dati memorizzati nella propria dotazione informatica. Per questo motivo è tenuto ad effettuare la copia di questi dati nel Server Documentale (Cartella di rete) messo a disposizione con la consapevolezza che tutto quello che non viene salvato sulla cartella documentale può essere perso in caso di danneggiamento dell'hard disk della postazione locale. Costituisce buona regola la periodica (almeno ogni mese) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.
7. Qualora fosse necessario, i backup e i relativi recuperi dei file verranno effettuati solo dall'infrastruttura di rete e non più da ulteriori dispositivi (es: USB, dischi esterni, DVD…).
8. Il personale preposto, nel caso: il Titolare del Trattamento, il DPO, il Garante o l'autorità giudiziaria effettuino un controllo sul documentale e prefiguri un uso improprio o che metta a repentaglio la sicurezza del sistema informatico dell'Ente, ha la facoltà, di procedere alla rimozione di ogni file o applicazione, nonché inibire temporaneamente l'accesso alle cartelle di rete interessate.
9. È fatto divieto applicare sistemi di crittografia, codificazione e simili ai dati se non espressamente richiesto dal Titolare secondo la tipologia di dato o documento.

CAPO IV - GESTIONE DELLE COMUNICAZIONI TELEMATICHE

Art. 13 - Utilizzo di Internet

1. L'utilizzo di Internet deve essere limitato a scopi inerenti all'attività lavorativa all'interno dell'Ente; ogni altro uso della navigazione Internet è assolutamente proibito;
2. È fatto divieto memorizzare dalla rete documenti, file o dati comunque non attinenti allo svolgimento delle attività aziendali, in particolare:
   a. non è consentito navigare in siti non attinenti allo svolgimento delle mansioni assegnate;
   b. non è consentita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo nei casi direttamente autorizzati dal titolare del trattamento e con il rispetto delle normali procedure di acquisto;
   c. è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;

d. non è permessa la partecipazione, per motivi non professionali, a Forum, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi (o nicknames) potendo esporre a rischi di sicurezza la rete aziendale;

3. Il Titolare del Trattamento si riserva di applicare appositi sistemi di URL filtering al fine di bloccare la navigazione su siti inseriti in "black list" ritenuti non conferenti con l'attività lavorativa e in applicazione a quanto disposto dalla normativa vigente ed in relazione a parametri valutativi quali sesso, droga, social media, acquisti online (amazon, e-price, ebay, ecc..);
4. Ogni necessità che si presentasse agli operatori di modificare l'URL filtering può essere motivatamente richiesta per iscritto dal Responsabile del Settore/Servizio al Titolare del Trattamento che, se l'istanza verrà valutata in modo positiva la richiesta verrà inoltrata al personale preposto che effettuerà la modifica;
5. Si rende noto che il comune ha attivato sistemi di monitoraggio della navigazione secondo le previsioni di cui al Provvedimento del Garante in materia di trattamento dati personali, Provvedimento del 1° marzo 2007 e del successivo regolamento (UE) 2016/679 effettuando monitoraggio generalizzato ed anonimo dei log di connessione.
6. Gli archivi di log risultanti da questo monitoraggio contengono traccia di ogni operazione di collegamento effettuata dall'interno della rete interna verso Internet. Eventuali attivazioni di controlli specifici saranno preventivamente notificate. I log di connessione di cui sopra, saranno conservati per i mesi previsti dalla normativa.
7. È fatto divieto all'utente il download di software freeware o shareware prelevato da siti Internet, di file musicali e video di qualsiasi genere scaricati dalla Rete o tramite software di tipo "peer to peer" se non espressamente autorizzato dall'Amministratore di Sistema;
8. È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa. È vietata la partecipazione a Forum non professionali, l'utilizzo di chat line, bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames);
9. Non è consentita la navigazione in siti ove sia possibile rilevare le opinioni politiche, religiose o sindacali dell'utilizzatore; non è consentito inoltre visitare siti e memorizzare documenti informatici di natura oltraggiosa e/o discriminatoria per sesso/etnia/religione/opinione e/o appartenenza sindacale e/o politica e/o filosofica;

Art. 14 - Gestione e utilizzo della posta elettronica

1. La casella di posta elettronica individuale istituzionale è assegnata agli Amministratori, al Segretario Generale, ai dipendenti assunti a tempo indeterminato e determinato ed ai collaboratori che, per le funzioni svolte, sono dotati di personal computer. Per particolari forme di lavoro, qualora le funzioni svolte richiedano l'uso della posta elettronica, la casella di posta elettronica individuale viene assegnata su espressa richiesta del Responsabile di riferimento;
2. La casella di posta elettronica assegnata è uno strumento di lavoro ed il suo utilizzo è consentito solo per finalità connesse allo svolgimento della propria attività lavorativa. Le persone assegnatarie sono responsabili del corretto utilizzo della stessa.
3. La posta elettronica diretta all'esterno della rete informatica aziendale può essere intercettata da estranei e, dunque, è preferibile non usarla per inviare documenti di lavoro "Strettamente Riservati", in questi casi è preferibile l'utilizzo della PEC.
4. È fatto divieto di utilizzare la casella di posta elettronica per:

a. trasmissione di dati sensibili, salvo i casi espressamente previsti dalla normativa vigente in materia di dati sensibili;
b. trasmissione di dati confidenziali e personali di alcun genere, salvo i casi espressamente previsti dalla normativa vigente in materia di protezione dei dati personali;
c. partecipazione a dibattiti, forum, o mailing-list non attinenti la propria attività o funzione svolta per l'Ente, salvo diversa ed esplicita autorizzazione.
d. non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica, o che costituiscano comunque condotta illecita;
e. non è consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, Forum, newsletter o mail-list, non attinenti all'attività lavorativa.

5. In caso di assenze dal lavoro programmate o non programmate, l'interessato può delegare un altro dipendente il quale provvederà a verificare il contenuto dei messaggi e ad inoltrare al titolare del trattamento quelli ritenuti rilevanti ed urgenti per lo svolgimento dell'attività lavorativa. In assenza di tale delega e, su richiesta scritta del Responsabile di Servizio, il personale preposto potrà accedere alla casella di posta elettronica dell'utente nei limiti previsti dall'art. 7 punto 9.
6. In caso di assenze dal lavoro programmate e per lungo periodo è buona norma attivare un risponditore automatico indicando una persona di riferimento alternativa con i relativi recapiti;
7. In caso di cessazione del rapporto di lavoro, il Responsabile del Servizio di afferenza dell'operatore interessato comunica al personale preposto la chiusura del rapporto lavorativo con l'utente, dopo tale comunicazione l'indirizzo di posta elettronica individuale dell'interessato sarà fornito di autorisponditore e mantenuto attivo per un periodo di tempo pari a quattro settimane successive alla chiusura del rapporto di lavoro. Dopo tale periodo il personale preposto sarà autorizzato a cancellare la Casella di Posta Istituzionale Personale.
8. È facoltà del personale incaricato, in funzione all'evoluzione tecnologica disponibile, di scegliere le applicazioni e le risorse che permettano di migliorare l'utilizzo della posta elettronica assegnata, tali applicazioni possono sostituire gli attuali software in uso ed essere utilizzate tramite i browser già installati nei PC comunali. Le caselle di posta elettronica istituzionali rientrano nell'ambito del patrimonio informativo dell'ente e pertanto seguiranno le stesse policy di sicurezza e back-up di cui ai punti precedenti.

Art. 15 - Utilizzo della rete e dei relativi servizi

1. La "rete" è l'insieme di servizi e apparecchiature tra di loro collegate attraverso cavi speciali che consentono agli utenti di utilizzare le risorse informatiche a prescindere dalla loro dislocazione nell'area della sede Municipale o delle sedi periferiche. Per evitare un possibile danneggiamento della rete è pertanto proibito collegare dispositivi informatici non autorizzati alla rete comunale, siano essi computer portatili, palmari, dispositivi WiFi o BlueTooth, smartphone ecc. Dette operazioni dovranno essere obbligatoriamente concordate con il personale preposto che autorizzerà o meno le operazioni richieste;
2. I servizi di rete e le unità di memorizzazione degli elaboratori presenti sono esclusivamente dedicati a scopi professionali e non possono in alcun modo essere utilizzate per fini diversi;
3. Le password d'ingresso alla rete e ai programmi sono segrete e vanno comunicate e gestite secondo le procedure suddette. È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente;

4. Se si rivelasse la necessità l'Amministratore di Sistema ha la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza o non pertinente l'attività lavorativa, sia sugli elaboratori sia sulle unità di rete, a cui seguirà comunicazione all'utente proprietario del file o utilizzatore del sistema su cui si è effettuato l'intervento;
5. È assolutamente vietato agli utenti:
   a. utilizzare strumenti che potenzialmente sono in grado di consentire l'accesso non autorizzato alle risorse informatiche (ad es. cracker, programmi di condivisione di file e programmi di chat, software di monitoraggio della rete in genere ecc.);
   b. Riconfigurare arbitrariamente i servizi già messi a disposizione in modo centralizzato, quali DNS e gateway;
   c. Intercettare pacchetti sulla rete, utilizzare sniffer o software di analisi del traffico dedicati a carpire dati personali, password e ID degli utenti o a controllare in qualunque modo le attività di rete;
6. Il personale preposto potrà utilizzare strumenti di monitoraggio del traffico di rete operando nel rispetto delle vigenti leggi in materia di riservatezza nella trattazione dei dati personali.

CAPO V - ASSISTENZA REMOTA

Art. 16 - Attività e strumenti di assistenza remota

1. Per teleassistenza si intende: l'azione di prendere il controllo di un PC senza personalmente recarsi nel luogo dove il PC è fisicamente posizionato. Per fare questo è necessario che il PC sia acceso e collegato alla rete informatica o tramite un apposito agente installato dal personale interno preposto o scaricando apposito software fornito e licenziato dalla ditta fornitrice del servizio assistenza.;
2. Per finalità di carattere manutentivo può essere utilizzato da parte del personale addetto un agente di assistenza remota che consenta di connettersi alle postazioni su esplicita richiesta degli utenti per fornire supporto in tempo reale e assistenza agli operatori nelle risoluzioni di problematiche di carattere informatico;
3. La connessione da remoto alla postazione dovrà essere esplicitamente autorizzata dall'utente.
4. Prima dell'attivazione del collegamento del soggetto esterno, il dipendente è tenuto a chiudere tutti i programmi attivi e file non attinenti all'applicazione per la quale è stata richiesta l'assistenza. Durante il collegamento, il dipendente non può abbandonare il posto di lavoro e deve verificare attentamente le operazioni che il soggetto incaricato collegato in remoto sta compiendo. Nel caso rilevi comportamenti scorretti o abusi, il dipendente è tenuto a chiudere immediatamente la connessione.
5. È facoltà del personale addetto l'utilizzo di software/agenti in grado di monitorare in tempo reale lo stato dei componenti hardware e software di ciascuna postazione in modo da garantire la tempestività di intervento in caso di anomalie e malfunzionamenti. Attraverso tale software sarà inoltre possibile la distribuzione di aggiornamenti del sistema operativo finalizzata alla correzione di vulnerabilità.
6. Il Software/agenti installati non dovranno in nessun caso permettere l'accesso e/o la visualizzazione di file e di dati contenuti nei Singoli PC da remoto, ma deve essere utilizzato solo ed esclusivamente per scopi tecnici e per effettuare: inventario hardware, software e di monitorare lo stato di salute della singola Macchina per permettere, nel limite del possibile, di anticipare l'assistenza prima che rotture e/o mal funzionamenti;

7. Questo software/agente sarà opportunamente dotato di funzionalità a supporto delle “Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015). (17A02399)”

CAPO VI - ABUSI, ATTIVITÀ VIETATE, CONTROLLI E RESPONSABILITÀ

art. 17 - Abusi e attività vietate

1. Si intende con abuso qualsiasi violazione del presente regolamento e di altre norme civili, penali e amministrative che disciplinano le attività e i servizi svolti sulla rete e di condotta personale.
2. È vietato ogni tipo di abuso. In particolare è vietato:
   - Usare la rete in modo difforme da quanto previsto dal presente regolamento.
   - Usare la rete in modo difforme da quanto previsto dalle leggi penali, civili e amministrative.
   - Utilizzare la rete comunale e quella internet per scopi incompatibili con l'attività istituzionale del Comune, fermi restando i casi successivamente disciplinati.
   - Utilizzare codici di accesso non propri.
   - Cedere a terzi i propri codici di accesso al sistema.
   - Conseguire l'accesso non autorizzato a risorse di rete interne o esterne al Comune di Porto Viro.
   - Agire con attività che influenzino negativamente la regolare operatività della rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti.
   - Agire con attività che distraggano risorse (persone, capacità, elaboratori).
   - Fare o permettere ad altri trasferimenti non autorizzati di informazioni (software, basi dati, ecc...)
   - Installare, eseguire o diffondere su qualunque dotazione informatica e sulla rete, programmi destinati a danneggiare o sovraccaricare i sistemi o la rete; come a titolo esemplificativo virus, cavalli di troia, worms, spamming della posta elettronica, programmi di file sharing.
   - Installare o eseguire programmi software non autorizzati e non compatibili con le attività istituzionali.
   - Cancellare, disinstallare, copiare, o asportare programmi software per scopi personali.
   - Installare componenti hardware non compatibili con le attività istituzionali
   - Rimuovere, danneggiare o asportare componenti hardware.
   - Utilizzare la posta elettronica inviando e ricevendo materiale che violi le leggi.
   - Accedere direttamente ad internet mediante strumenti non autorizzati.
   - Connettersi ad altre reti, pubbliche o private, senza autorizzazione.
   - Leggere, copiare o cancellare files e software di altri utenti, senza averne l'autorizzazione esplicita.
   - Usare l'anonimato o servirsi di risorse che consentano di restare anonimi.
   - Inserire o cambiare password del bios, se non dopo averla espressamente comunicata all'Amministratore di sistema e essere stati espressamente autorizzati.
   - Abbandonare il posto di lavoro lasciandolo collegato alla rete senza il blocco del salva schermo (attivabile anche attraverso i tasti CTRL+ALT+CANC blocca computer).

Art. 18 - Controlli e responsabilità

1. L'Amministrazione si riserva di effettuare controlli sul corretto utilizzo degli strumenti informatici e telematici nel rispetto del presente regolamento e delle normative vigenti in materia di privacy e dei diritti dei lavoratori;

2. Per motivi di sicurezza e protezione dei dati, ogni attività di monitoraggio compiuta nella rete Informatica può essere sottoposta a registrazione in appositi file. Detti file 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 delle norme vigenti.
La riservatezza delle informazioni è soggetta a quanto dettato dal D. Lgs. 196/2003 e s.m.i. e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori. Tali controlli saranno mirati ad individuare eventi dannosi o situazioni di pericolo per le quali non sia stato possibile impedirne gli effetti attraverso preventivi accorgimenti tecnici;

3. Qualora, durante un controllo generalizzato, vengano rilevate anomalie nell'utilizzo degli strumenti informatici, l'Amministrazione provvederà ad inviare al personale preposto preliminarmente un avviso generalizzato relativo all'uso improprio riscontrato, con l'invito ad attenersi scrupolosamente al presente Regolamento. Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie;

4. Il mancato rispetto o la violazione delle norme contenute nel presente Regolamento è perseguibile con provvedimenti disciplinari, nonché con le azioni civili e penali consentite.

CAPO VII - AGGIORNAMENTO E REVISIONE, SANZIONI E DEROGHE

Art. 19 - Aggiornamento e revisione

1. Tutti gli utenti possono proporre integrazioni e osservazioni motivate al presente Regolamento indirizzandole al proprio Responsabile incaricato, il quale potrà inoltrarle al personale preposto. Le proposte verranno esaminate dal DPO, dal Titolare del trattamento, al Responsabile del trattamento dei dati che darà apposite indicazioni all'Amministratore di Sistema.
2. Il presente Regolamento è soggetto a revisione ogniqualvolta se ne manifesti la necessità o in funzione dell'evolversi della configurazione del Sistema Informatico comunale e della normativa in materia.
3. Per qualsiasi dubbio relativo all'applicazione pratica o all'interpretazione del presente regolamento, il dipendente può rivolgersi al Titolare del trattamento o al responsabile protezione dei dati.

Art. 20 - Sanzioni e deroghe

1. È fatto obbligo a tutti gli utenti di osservare le disposizioni portate del presente Regolamento, ad eccezione delle manifeste necessità e dei casi attestati e motivati da parte dell'utente interessato e autorizzati dal Responsabile Preposto.

2. Il mancato rispetto e/o la violazione delle regole sopra riportate sarà comunicato al Servizio del Personale il quale provvederà ad attuare i necessari provvedimenti disciplinari e/o risarcitori previsti dai vigenti CC.CC.NN.LL., nonché con tutte le azioni civili e penali consentite dalle vigenti norme.

CAPO VIII – LINEE GUIDA AGID

Art. 21 - Implementazione delle linee AGID nel Comune

AGID è l'Agenzia per l'Italia Digitale: l'agenzia tecnica della Presidenza del Consiglio che ha il compito di garantire la realizzazione degli obiettivi e di contribuire alla diffusione dell'utilizzo delle tecnologie dell'informazione e della comunicazione, favorendo l'innovazione e la crescita economica.

Il Comune di Porto Viro sta implementando ed adeguando l'I.T.C alle linee guida AGID: 17 marzo 2017, n. 1/2017: "Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015). (17A02399)"

Tali linee guida (allegato n. 3) hanno lo scopo di garantire nel limite del possibile la sicurezza informatica dell'Ente sia a livello ITC e sia a livello, molto più importante, di tutelare il dato come patrimonio del Comune di Porto Viro.

CAPO IX - Lavoro agile e sicurezza dei dati personali

Art. 22 - Le 10 raccomandazioni di AgID per uno Smart working sicuro

- 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 email 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.

Art. 23 - Indicazioni generali

1. Non stampare documentazione riservata da casa se non autorizzati;
2. salvare documenti sul pc personale solo temporaneamente e poi cancellarli appena esaurita la finalità per cui è stato necessario eseguire l'operazione;
3. porre attenzione nell'inviare foto per provare che si è in smart working quando sul monitor vi sono dati personali;
4. l'accesso a dati aziendali non è più pericoloso in smart working, la pericolosità dipende da come lo strumento e l'operatore gestiscono il dato, non dalla locazione della persona

Art. 24 - Requisiti minimi di sicurezza informatica su computer personali che devono accedere esclusivamente al software gestionale del comune via browser Web (no client/server)

1. assicurarsi di avere una buona connessione ad Internet (nel caso di connessioni scadenti si possono verificare corruzione dei dati);
2. controllare che il sistema operativo in uso sia aggiornato (Windows > 8.1, Mac > Sierra);
3. Impostare una password di accesso al computer;
4. il pc deve essere ad uso esclusivo del dipendente (non utilizzato dai familiari);
5. utilizzare un Antivirus (non free) del tipo Internet Security (firewall integrato) e verificare che sia aggiornato;
6. Il computer deve avere installato solo i programmi necessari all'operatività aziendale (no programmi torrent, programmi non originali, programmi che possano registrare l'attività dell'utente, ecc.). A titolo indicativo e non esaustivo i programmi consentiti sono:
   a. Strumenti Produttività
      i. Open Office, Libre Office, Microsoft Office
   b. Browser Web
      i. Google Chrome, Firefox
   c. Utilità
      i. Acrobat Reader, 7zip
7. Mantenere riservate le password di accesso al gestionale e non memorizzarle all'interno del browser web;
8. Eseguire sempre il log out quando si intende uscire dalla procedura gestionale.

Art. 25 - Requisiti aggiuntivi nel caso di accesso da parte del dipendente attraverso il proprio computer a materiale che si trova nel server/NAS del comune

1. Instaurare una connessione VPN protetta tra il computer e la sede dell'Ente
   a. Una VPN (Virtual Private Network) consente di creare una rete privata virtuale che garantisce privacy, anonimato e sicurezza dei dati attraverso un canale di comunicazione riservato tra dispositivi dislocati nel territorio.
   b. Indipendentemente dalla tipologia VPN usata (accesso remoto/site-to-site) per instaurare una connessione tra un client ed il relativo server i passi che sono richiesti possono essere così riassunti:
      - il client contatta il server;
      - il server notifica la propria presenza;
      - il client richiede al server di essere identificato;
      - il server verifica che il tentativo di connessione sia autorizzato previa autenticazione riuscita;
      - il server risponde alla richiesta di autenticazione e autorizza la comunicazione con il client;
      - inizia la comunicazione tra le due entità.
   2. Le credenziali per l'accesso alla VPN devono essere comunicate solo al dipendente.
   3. Il comune deve tenere traccia degli accessi effettuati dai dipendenti attraverso un sistema di Log.

Art. 26 - Utilizzo programmi di controllo remoto

Per i comuni che intendono avere la massima operativa e sicurezza senza la necessità di imporre prerequisiti ai computer personali dei dipendenti raccomando l'acquisto di software che permettano il controllo remoto della postazione di lavoro dell'ufficio. (Supremo, TeamViewer, AnyDesk, ecc.).

Il software scelto dal Comune di Porto Viro è LiveCare che oltre a permettere la connessione da remoto al proprio PC garantisce canoni di sicurezza ed una registrazione di log di connessione alla postazione di riferimento.
Un software di controllo remoto LiveCare è un programma grazie al quale, con una connessione internet e una password, si può accedere ad un altro computer operandovi come se si fosse in ufficio.
Vantaggi di questa soluzione:

1. Facile implementazione (basta installare un programma)
2. Il computer che si connette dall'esterno al comune è separato dal desktop remoto quindi non c'è promiscuità fra i 2 sistemi
3. La connessione è crittografata