ALLEGATO A

REGOLAMENTO

SULLE MODALITÀ D'USO DELLE RISORSE INFORMATICHE E DI ALTRI STRUMENTI DI LAVORO E SULLE MISURE MINIME E IDONEE DI SICUREZZA PER IL TRATTAMENTO DEI DATI

PREMESSA....1
ART. 1 OGGETTO....1
ART. 2 INDIVIDUAZIONE DEI RUOLI DI RESPONSABILITÀ....2
ART. 3 INTERESSI E RISCHI DELL'ENTE E DEI DIPENDENTI, AMMINISTRATORI E COLLABORATORI DELL'ENTE....2
ART. 4 UTILIZZO DELLE RISORSE INFORMATICHE E DI ALTRI STRUMENTI DI LAVORO IN DOTAZIONE....3
ART. 5 MODALITÀ DI UTILIZZO DELLE RISORSE INFORMATICHE....3
ART. 6 ACCESSO AI SISTEMI INFORMATIVI DELL'ENTE – LE CREDENZIALI....4
ART. 7 IL SISTEMA DI MEMORIZZAZIONE DEGLI OGGETTI INFORMATICI....6
ART. 8 IL SISTEMA DI POSTA ELETTRONICA....6
ART. 9 LA NAVIGAZIONE INTERNET....8
ART. 10 LE APPLICAZIONI INFORMATICHE SPECIALISTICHE....9
ART. 11 USO DEI TELEFONI FISSI E DEI FAX....9
ART. 12 USO DEI DISPOSITIVI MOBILI....9
CAPO II ISTRUZIONI E MISURE DI SICUREZZA PER IL TRATTAMENTO DEI DATI A CUI SI DEVONO ATTENERE GLI INCARICATI....10
ART. 13 DEFINIZIONE DI TITOLARE, RESPONSABILE E INCARICATO DEL TRATTAMENTO DEI DATI PERSONALI....10
ART. 14 TRATTAMENTO DEI DATI EFFETTUATO CON STRUMENTI ELETTRONICI O COMUNQUE AUTOMATIZZATI....10
ART.15 TRATTAMENTO DEI DATI CON STRUMENTI DIVERSI DA QUELLI ELETTRONICI O COMUNQUE AUTOMATIZZATI……..12
ART. 16 RESPONSABILITÀ IN CASO DI VIOLAZIONE DELLE ISTRUZIONI……12
ART. 17 CONFIDENZIALITÀ DEI DATI PERSONALI TRATTATI....13
ART. 18 PRECAUZIONI DA ADOTTARE NEL TRATTAMENTO DEI DATI CONTENUTI IN ARCHIVI E DOCUMENTI CARTACEI....13
ART. 19 PRECAUZIONI SPECIFICHE PER I RAPPORTI DI FRONT-OFFICE....14
ART. 20 PRECAUZIONI DA ADOTTARE NEL TRATTAMENTO DEI DATI CONSEGUENTI ALL'ATTIVITÀ DI VIDEOSORVEGLIANZA....15
ART. 21 PRECAUZIONI DA ADOTTARE PER LA TUTELA DELLA SICUREZZA DEL SISTEMA INFORMATICO COMUNALE....15
ART. 22 PRECAUZIONI DA ADOTTARE NELL'UTILIZZO DELLA POSTA ELETTRONICA IN ORDINE AL TRATTAMENTO DEI DATI....16
ART. 23 PRECAUZIONI DA ADOTTARE NELLA NAVIGAZIONE IN INTERNET IN ORDINE AL TRATTAMENTO DEI DATI....18
CAPO III DISPOSIZIONI FINALI....19
ART. 25 PRIORITÀ DELLE MISURE TECNICHE DI PROTEZIONE....19
ART. 26 COMPITI DI SORVEGLIANZA....19
ART. 27 GRADUALITÀ DEI CONTROLLI....19
ART. 28 DISTINZIONE TRA E-MAIL PRIVATE ED E-MAIL PROFESSIONALI....21
ART. 29 OBBLIGATORIETÀ OSSERVANZA DISPOSIZIONI E SANZIONI....21
ART. 30 DISPOSIZIONI ULTERIORI....21
ART. 31 ESERCIZIO DEI DIRITTI EX ART. 7 D.LGS. 196/2003....22
ART. 32 DISPOSIZIONI DI RINVIO....22
CLASSIFICAZIONE DEI SISTEMI DI ARCHIVIAZIONE E DI TRATTAMENTO DEI DATI E MISURE MINIME DI SICUREZZA DA ADOTTARE AI SENSI DEL D. LGS. 196/2003....23

PREMESSA

Il Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione di dati personali" e l'Allegato Disciplinare Tecnico impongono comportamenti tali da assicurare a chiunque il diritto alla protezione dei dati personali che lo riguardano, e l'adozione di misure di sicurezza minime e di misure di sicurezza idonee a garantire tale diritto, rispettivamente disciplinate dall'art. 33 e dall'art. 31 del Codice.
Il Garante per la protezione dei dati personali ha inoltre emanato, in data 01/03/2007, un provvedimento in materia di lavoro ("*Lavoro: le linee guida del Garante per Posta Elettronica e Internet*") con il quale prescrive ai datori di lavoro di adottare la "misura necessaria", a garanzia degli interessati, riguardante l'onere di specificare le modalità di utilizzo della Posta Elettronica e della rete Internet da parte dei lavoratori, come successivamente indicato anche nella Direttiva n. 02/2009 della Presidenza del Consiglio dei Ministri – Dipartimento della Funzione Pubblica.
Il Comune di Verona, come Ente e in qualità di Datore di Lavoro, in un'ottica di trasparenza e correttezza, integrando quanto già indicato nel Regolamento sulle modalità d'uso delle risorse informatiche, sul loro utilizzo telematico e sulle misure minime di sicurezza per il trattamento dei dati, approvato con D.G. n. 456 del 16/08/2000, modificato con D.G. n. 89 del 26/08/2008 di approvazione del Documento Programmatico sulla Sicurezza (DPS), e successivamente oggetto di modifiche ed integrazioni, e altresì recependo alcune disposizioni contenute nel Disciplinare della Regione del Veneto per l'utilizzo di Posta Elettronica, Internet, Telefoni e Fax all'interno di Regione del Veneto, ALLEGATO A alla Dgr n. 863 del 31/03/2009, adotta il presente Regolamento per disciplinare il corretto utilizzo degli strumenti di lavoro e soprattutto delle risorse informatiche in dotazione a dipendenti, amministratori e collaboratori così come le misure di sicurezza idonee a garantire la protezione dei dati da esso trattati, in aggiunta alle misure di sicurezza minime, al fine di assicurare il corretto espletamento delle funzioni dell'Ente e la liceità dell'attività svolta da dipendenti, amministratori e collaboratori.
Nel presente Regolamento si è infine tenuto conto della posizione assunta dal Garante per la protezione dei dati personali con il provvedimento n. 456 del 30/07/2015 in materia di gestione dell' e-mail aziendale, a conclusione del rapporto di lavoro, e del Decreto Legislativo sul lavoro e pari opportunità, attuativo della Legge 183/2014 Deleghe al Governo in materia di riforma degli ammortizzatori sociali, dei servizi per il lavoro e delle politiche attive, nonché in materia di riordino della disciplina dei rapporti di lavoro e dell'attività' ispettiva e di tutela e conciliazione delle esigenze di cura, di vita e di lavoro (cd. Jobs Act).

ART. 1 - OGGETTO

1.1 Il presente Regolamento disciplina:

a) le modalità di utilizzo delle risorse informatiche e di altri strumenti di lavoro nell'ambito dello svolgimento delle proprie mansioni, dei propri compiti di lavoro e nelle attività di ufficio da parte dei dipendenti, a qualsiasi titolo inseriti nell'organizzazione comunale, nonché degli amministratori e dei collaboratori dell'Ente, a prescindere dal rapporto contrattuale intrattenuto con lo stesso che, per quanto riguarda le risorse informatiche, hanno in dotazione almeno una credenziale di accesso al sistema informatico comunale e/o almeno una stazione di lavoro di tipo personal computer in grado di accedere al sistema informatico comunale;

b) l'individuazione del complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione per il trattamento dei dati aziendali e personali, al fine di:

- garantire l'aderenza e la rispondenza alle vigenti normative in materia e gli adeguati livelli di sicurezza ed integrità del patrimonio informativo dell'Amministrazione comunale;
- stabilire le istruzioni operative e le misure di sicurezza a cui devono attenersi gli incaricati del trattamento, informandoli riguardo le norme nazionali vigenti e le disposizioni dell'Ente relativamente all'utilizzo delle risorse informatiche e degli altri strumenti di lavoro;

c) le modalità con le quali possono essere effettuati controlli sull'uso delle risorse informatiche e degli altri strumenti di lavoro, nell'interesse dell'Ente e nel rispetto della riservatezza dei dati personali di dipendenti, amministratori e collaboratori relativamente all'uso di Posta Elettronica, Internet e telefoni altri strumenti tecnologici aziendali.

ART. 2 - INDIVIDUAZIONE DEI RUOLI DI RESPONSABILITÀ

2.1 Ai fini del presente regolamento:

α) per "TITOLARE" si intende l'Ente Comune di Verona cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati, ivi compreso il profilo della sicurezza;

β) per "STRUTTURA" si intendono le Unità Organizzative individuate dal Comune di Verona e dirette da un Dirigente.

χ) per "AMMINISTRATORE DI SISTEMA" si intende il soggetto cui è conferito il compito di sovrintendere alle risorse del sistema informatico;

δ) per "RESPONSABILE" si intende il soggetto che, per collocazione funzionale, esperienza, capacità e affidabilità assume il compito di garantire il rispetto delle vigenti disposizioni in materia di trattamento dati, ivi compreso il profilo relativo alla sicurezza;

ε) per "INCARICATO DEL TRATTAMENTO" si intende il soggetto che è stato autorizzato dal titolare o dal responsabile a compiere operazioni sui dati cui ha accesso.

ART. 3 - INTERESSI E RISCHI DELL'ENTE E DEI DIPENDENTI, AMMINISTRATORI E COLLABORATORI DELL'ENTE

3.1 Nel luogo di lavoro va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità di dipendenti, amministratori e collaboratori dell'Ente, in un'ottica di reciproci diritti e doveri.

3.2 Gli strumenti di lavoro e in particolare le risorse informatiche e telematiche, messi a disposizione dall'Ente ai dipendenti, amministratori e collaboratori, devono essere utilizzati in modo responsabile e ispirato ai principi di diligenza e correttezza. Essendo di proprietà dell'Ente, devono essere utilizzati per il conseguimento dei suoi fini istituzionali e non per scopi diversi. Non vengono rilasciate copie o autorizzazioni di utilizzo di applicazioni o componenti software, licenziati a nome dell'Ente, per scopi privati, ed è inoltre fatto divieto di utilizzare le risorse informatiche comunali per comunicare in modo anonimo o modificando la reale identità del mittente.

3.3 Per l'Ente l'utilizzo improprio, da parte di dipendenti, amministratori e collaboratori, di Posta Elettronica, Internet e telefoni o altri strumenti tecnologici aziendali, può pregiudicare il regolare funzionamento delle installazioni tecniche o altri beni o interessi meritevoli di tutela e/o giuridicamente protetti, tra cui:
a)economie dei costi;

b)la capacità di memoria utilizzabile dei server o l'ampiezza di banda disponibile per il collegamento in rete;
c)sicurezza delle applicazioni e dei dati (*disponibilità*, *integrità*, cd. *confidenzialità*);
d)produttività sul lavoro;
e)la reputazione o l'immagine dell'Amministrazione comunale;
f)responsabilità oggettiva dell'Amministrazione comunale, ex art. 2049 c.c., per comportamenti illeciti dei propri dipendenti.

3.4 Per dipendenti, amministratori e collaboratori dell'Ente, i rischi derivanti dall'utilizzo di Posta Elettronica, Internet e telefoni o altri strumenti tecnologici aziendali, riguardano:
a)la protezione dei dati personali, propri e di terzi, poiché i predetti strumenti lasciano "tracce" del loro uso;
b)la possibilità che l'Ente, in fase di eventuale legittimo controllo, venga a conoscenza di dati od opinioni personali di dipendenti, amministratori e collaboratori;
c)relativamente all'uso di Posta Elettronica, di Internet, e di supporti rimovibili l'introduzione di virus, worm, cavalli di Troia o installazioni di programmi estranei nel computer utilizzato da dipendenti, amministratori e collaboratori, con conseguente perdita di tutti o parte dei file salvati sul medesimo computer.

CAPO I

UTILIZZO DI RISORSE INFORMATICHE E ALTRI STRUMENTI DI LAVORO

ART. 4 – UTILIZZO DELLE RISORSE INFORMATICHE E DI ALTRI STRUMENTI DI LAVORO IN DOTAZIONE

4.1 Risorse informatiche e altri strumenti di lavoro vengono forniti in dotazione dall'Amministrazione comunale esclusivamente per lo svolgimento dell'attività lavorativa o istituzionale.
Si intende per risorsa informatica una qualsiasi combinazione di apparati tecnologici, hardware o software, utilizzati per le comunicazioni elettroniche ed elaborazione dei dati, laddove la comunicazione elettronica è una qualsiasi notizia creata, inviata, inoltrata, trasmessa, archiviata, copiata, scaricata, mostrata, vista o stampata da uno o più sistemi o servizi di comunicazione elettronica.
A dipendenti, amministratori e collaboratori vengono forniti inoltre in dotazione altri strumenti di lavoro, quali telefoni, cellulari, fax, scanner, etc.

ART. 5 – MODALITÀ DI UTILIZZO DELLE RISORSE INFORMATICHE

5.1 Durante l'espletamento della propria attività gli INCARICATI DEL TRATTAMENTO dei dati, che sono dotati di strumentazione informatica idonea, devono attenersi alle seguenti disposizioni:

NON È CONSENTITA:

- l'installazione e la duplicazione di software non coperto da regolare licenza fornita dalla STRUTTURA di appartenenza;
- l'installazione di software libero non soggetto a licenza d'uso, non autorizzato dalla STRUTTURA di appartenenza o dall'AMMINISTRATORE DI SISTEMA;

- l’installazione di software non autorizzato, finalizzato ad alterare la funzionalità del collegamento in rete della stazione di lavoro;
- l’alterazione degli indirizzi e dei protocolli di rete assegnati dall’AMMINISTRATORE DI SISTEMA;
- l’inibizione o la sospensione, anche temporanea, del funzionamento del software ANTIVIRUS installato dall’AMMINISTRATORE DI SISTEMA;
- l’utilizzazione di funzioni e tecniche di condivisione di archivi gestiti dalla propria postazione di lavoro senza la contemporanea adozione di opportune parole chiave di accesso (password) da fornire ai colleghi che ne debbano fare uso;
- il trasferimento di dati non autorizzato da e verso l’esterno alla Amministrazione Comunale in qualsiasi forma (supporti dati rimovibili, collegamento linee dati con o senza fili, utilizzo di reti telematiche private o pubbliche, ecc.);
- l'attivazione della protezione hardware per bloccare la postazione di lavoro in dotazione.

È OBBLIGATORIA:

- l’utilizzazione di tutte le cautele riguardanti l’uso di software del quale non si conoscano appieno le potenzialità;
- l’attività di aggiornamento del proprio software ANTIVIRUS ad ogni connessione alla rete telematica, segnalando tempestivamente all’amministratore del sistema (Direzione Informatica e-Government, di seguito denominata Direzione Informatica) se la propria postazione di lavoro non è stata collegata alla rete comunale per periodi superiori ai 30 giorni solari;
- la denuncia e registrazione di archivi informatici presenti sulla propria stazione di lavoro, ai sensi del Codice in materia di protezione dei dati personali, nonché l’applicazione di tutte le norme conseguenti alla gestione e mantenimento di tali informazioni regolarmente autorizzata;
- la comunicazione alla STRUTTURA di appartenenza dell’insorgere di condizioni anomale che possono comportare una non perfetta aderenza alle norme di comportamento indicate nel presente regolamento.
- l’installazione dei certificati di postazione lavoro solo su postazioni client degli utenti autorizzati.

ART. 6 – ACCESSO AI SISTEMI INFORMATIVI DELL’ENTE – LE CREDENZIALI

6.1 Le credenziali (tipicamente di tipo user e password) che i soggetti autorizzati hanno in dotazione per l’espletamento della propria attività, e che permettono l’accesso ai sistemi informatici comunali o nella disponibilità dell'Ente, sono da considerarsi **strettamente riservate**.

6.2 Per i sistemi che, per la natura dei dati che trattano, prevedono credenziali di tipo personale, i soggetti autorizzati devono adottare la massima cura perché la password non sia in alcun modo ceduta a terzi.

6.3 Le password delle credenziali, per le quali è prevista una scadenza periodica, devono essere tempestivamente cambiate secondo le regole stabilite dall’AMMINISTRATORE DI SISTEMA. Per gli utenti esterni le credenziali vengono fornite con scadenza massima non superiore all'anno.

6.4 Le credenziali sono rilasciate a soggetti con rapporto regolato da condizioni contrattuali che stabiliscono responsabilità e diritti di fronte alla legge (carica elettiva, rapporto di lavoro continuativo o a tempo determinato, contratto di consulenza, etc.) o a soggetti esterni appartenenti ad Enti o Aziende che intrattengono rapporti con il Comune di Verona.

6.5 Le credenziali sono rilasciate su richiesta del Dirigente della STRUTTURA o dell'Ente o Azienda cui l'interessato appartiene, su autorizzazione del RESPONSABILE della base-dati cui il trattamento specifico fa riferimento.

6.6 Le credenziali sono revocate o sospese quando l'attività per la quale le credenziali sono state richieste, rispettivamente cessa o è temporaneamente sospesa e comunque alla cessazione del rapporto con il TITOLARE (Comune di Verona), come evidenziato nella tabella sottostante relativa alla gestione delle credenziali per l'accesso a intranet (credenziale IDM), applicativi con credenziali IDM, ulteriori applicativi con altre credenziali, e posta elettronica.

tipologia	intranet IDM	applicativi con credenziali IDM	ulteriori applicativi con altre credenziali	posta elettronica
cessazione rapporto di lavoro a tempo indeterminato / tempo determinato	no	no	no	· nessun accesso · conservazione dati per 60 giorni dalla data di cessazione · avviso automatico al mittente di chiusura della casella
cessazione somministrazione lavoro	no	no	no	· nessun accesso · conservazione dati per 60 giorni dalla data di cessazione · avviso automatico al mittente di chiusura della casella
cessazione co.co.co / stagisti /incarichi esterni / incarichi gratuiti	no	no	no	· nessun accesso · conservazione dati per 60 giorni dalla data di cessazione · avviso automatico al mittente di chiusura della casella
sospensione disciplinare (per almeno 15 giorni)	no	no	no	- nessun accesso - conservazione dati - avviso automatico al mittente di chiusura della casella
comando/distacco presso altro ente	no	no	no	- nessun accesso - conservazione dati - avviso automatico al mittente di chiusura della casella
assenze, aspettative o part-time ciclico	si	si	si	- si

ART. 7 – IL SISTEMA DI MEMORIZZAZIONE DEGLI OGGETTI INFORMATICI

7.1 Il sistema gestisce due tipi di memoria elettronica: la *"memoria personale"* e la *"memoria di struttura"*

7.2 Della porzione di "*memoria personale",* che va utilizzata per finalità lavorative o istituzionali, è responsabile l'intestatario dell'utenza.

7.3 La "*memoria personale"* viene utilizzata per memorizzare dati ritenuti utili dall'intestatario, per esigenze connesse alla propria attività.

7.4 Le porzioni di memoria denominate *"memoria di struttura"* sono assegnate a ciascuna STRUTTURA nella persona del Dirigente che la dirige che assume il ruolo di RESPONSABILE dei dati ivi contenuti.

7.5 Il RESPONSABILE ha la piena disponibilità degli archivi elettronici della propria STRUTTURA. Egli, in base alle esigenze della propria organizzazione, "suddivide" la memoria in "porzioni" cui abilitare i propri collaboratori, quali INCARICATI DEL TRATTAMENTO dei dati, in differenti modalità (sola lettura, scrittura) in base alle esigenze organizzative (per gruppi, singolarmente, etc.)

7.6 Il RESPONSABILE assegna agli INCARICATI DEL TRATTAMENTO credenziali di tipo personale.

7.7 Il RESPONSABILE può in qualsiasi momento accedere all'intero contenuto della memoria assegnata alla propria STRUTTURA per verificarne sia il corretto utilizzo che la necessità di conservarne gli oggetti presenti nel tempo.

ART. 8 – IL SISTEMA DI POSTA ELETTRONICA

8.1 Le Caselle di Posta elettronica sono di due tipi: "*caselle personali"* e "*caselle di struttura*", certificate o no.

8.2 Della "*casella personale",* che va utilizzata per finalità lavorative o istituzionali, è responsabile l'intestatario.

8.3 La gestione della "*casella personale"* ha un ruolo vitale nelle politiche di sicurezza delle procedure informatiche: infatti, essendo il dialogo della posta di tipo sicuro (https criptato) ed essendo la password con cui si utilizza la posta di tipo personale non cedibile, la casella può essere utilizzata anche per comunicare ad un collega un elemento particolarmente critico, come ad esempio una password o un link di attivazione (ovviamente non la password IDM) per via telematica.

8.4 La *"casella personale"* è assoggettata al segreto postale e pertanto di uso esclusivo dell'intestatario. Le registrazioni effettuate sono fatte ai sensi di legge solo per eventuale utilizzo da parte dell'Autorità Giudiziaria.

8.5 L'intestatario di una "casella di struttura" è il Dirigente che la dirige. Egli assume il ruolo di RESPONSABILE.

8.6 Il RESPONSABILE di una "casella di struttura" comunica agli INCARICATI DEL TRATTAMENTO dei dati, la password di accesso in base alle esigenze organizzative della propria STRUTTURA.

8.7 Il RESPONSABILE verifica periodicamente il corretto utilizzo della "casella di struttura", provvede al cambio periodico della password di accesso e all'aggiornamento della lista degli INCARICATI DEL TRATTAMENTO.

8.8 La Posta Elettronica che l'Amministrazione comunale mette a disposizione deve essere utilizzata in modo pertinente allo svolgimento dell'attività lavorativa o istituzionale, secondo un utilizzo appropriato, efficiente, corretto e razionale nel rispetto del principio di riservatezza. Gli intestatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse. I dirigenti sono responsabili delle caselle di posta di struttura assegnate alle rispettive Unità organizzative.

8.9 Gli intestatari delle caselle sono tenuti, in un'ottica di correttezza ed uso responsabile degli strumenti, a contribuire alla riduzione del fenomeno dello "spam" (trasmissione su larga scale e in grandi volumi di e-mail non sollecitati), evitando di rispondere e/o inviare ad altri destinatari eventuali messaggi, del tipo "catene di Sant'Antonio", non sollecitati, che siano stati ricevuti, ed evitando di comunicare ad altri destinatari, in modo indiscriminato, il proprio indirizzo di posta elettronica o quello di colleghi.

8.10 È fatto divieto di utilizzare le caselle di posta elettronica del dominio dell'Amministrazione comunale ("comune.verona.it") per motivi diversi da quelli strettamente legati all'attività lavorativa o istituzionale.

8.11 Solo in caso di necessità e urgenza, gli intestatari delle caselle possono utilizzare la Posta Elettronica per motivi non attinenti all'attività lavorativa o istituzionale e, comunque, non in modo ripetitivo. In tali limitati casi, le e-mail personali è opportuno che siano contrassegnate con la menzione "Privato" o "Riservato" all'inizio dell'oggetto.

8.12 Ove possibile, ai fini di una migliore differenziazione tra e-mail private o riservate ed e-mail professionali, gli intestatari delle caselle potranno chiedere ai mittenti che eventuali e sporadici messaggi privati o riservati siano inviati con la dicitura "Privato" o "Riservato" nell'oggetto. Relativamente alla distinzione tra e-mail private ed e-mail professionali, si rimanda inoltre al successivo art. 28 del presente Regolamento.

8.13 Nonostante la corrispondenza elettronica possa essere archiviata fino al raggiungimento di un determinato spazio di memoria assegnato ad ognuno, gli intestatari delle caselle sono tenuti a mantenere in ordine la casella di posta loro assegnata, eliminando i documenti e gli allegati obsoleti e/o inutili.

8.14 In caso di cessazione dell'attività lavorativa o istituzionale, l'account di Posta Elettronica del dipendente nonché dell'amministratore e del collaboratore dell'Ente è prontamente disabilitato e la sua casella di Posta Elettronica estinta. Prima della cancellazione gli interessati possono richiedere il salvataggio dei messaggi "privati" o "riservati" di Posta Elettronica su supporti di dati privati.

8.15 I mittenti di e-mail inviati all'indirizzo e-mail disabilitato vengono informati che l'indirizzo del destinatario è estinto al momento della cancellazione dell'account.

ART. 9 - LA NAVIGAZIONE INTERNET

9.1 L'autorizzazione alla navigazione internet di un proprio collaboratore è effettuata dal Dirigente di riferimento.

9.2 La navigazione avviene attraverso una Credenziale Personale, è registrata e risponde ai requisiti di sicurezza necessari per evitare usi impropri del servizio.

9.3 Tutte le registrazioni sono fatte mantenendo la privacy dell'utente e vengono distrutte periodicamente, utilizzabili solo per necessità dell'autorità giudiziaria ai sensi di legge.

9.4 Per quanto riguarda l'accesso ai siti Internet si adottano le seguenti procedure:

a) distribuzione di norme interne di comportamento dei dipendenti previste dal D.P.R. 62/2013 *Regolamento recante Codice di comportamento dei dipendenti pubblici, a norma dell'art. 54 del decreto legislativo 30 marzo 2001, n. 165* e approvate con D.G. n. 49/2014, le cui disposizioni generali anche in materia di anticorruzione sono da applicarsi a tutto il personale a tempo indeterminato, determinato, collaboratori o consulenti con qualsiasi tipologia di contratto o incarichi e a qualsiasi titolo, ai titolari di organi e di incarichi negli uffici di diretta collaborazione delle autorità politiche, nonché nei confronti dei collaboratori a qualsiasi titolo di imprese fornitrici di beni o servizi e che realizzano opere in favore dell'amministrazione;

b) evidenziazione a video del divieto di accesso a siti non autorizzati;

c) verifica a campione degli accessi con modalità che escludano l'identificazione di persone eventualmente contattate;

d) installazione di software-filtro che permettano di inibire o restringere l'accesso a siti non autorizzati e/o limitare i tempi di collegamento.

9.5 Considerato che Internet è uno strumento di utilità per l'Amministrazione comunale, oltre che per la crescita professionale del singolo dipendente e collaboratore, l'accesso ad Internet deve essere utilizzato in modo strettamente pertinente allo svolgimento dell'attività lavorativa o istituzionale, secondo un utilizzo appropriato, efficiente, corretto e razionale.

9.6 È fatto divieto di navigare in Internet per motivi diversi da quelli legati alla propria attività. I dipendenti, amministratori e collaboratori, in particolare, sono tenuti a utilizzare Internet per le specifiche finalità della propria attività e non devono inoltre appesantire il traffico della rete con collegamenti particolarmente lunghi e complessi (es. *download* di file, connessioni a stazioni radio on line, applicazioni "*peer to peer*", chat, Skype o similari,, etc.) quando ciò non sia collegato allo svolgimento della propria attività.

9.7 I dipendenti, amministratori e collaboratori, durante l'orario della propria attività, possono accedere liberamente alle pagine della rete Intranet e inoltre accedere ai siti Internet eventualmente pubblicizzati nelle pagine Intranet, nel rispetto di quanto disposto al comma 5 del presente articolo, essendo a cura dell'Amministrazione comunale proporre i siti Internet, anche di natura divulgativa, che possono essere utili all'espletamento della propria attività.

9.8 Per le sedi comunali ove esistono provvisoriamente connessioni internet dirette cioè non gestite dal sistema informatico comunale, la responsabilità sull'utilizzo e sull'accesso alla rete Internet è a carico del responsabile dell'ufficio cui è stato affidato il collegamento

(tipicamente di tipo ADSL). Egli può delegarne l'utilizzo a propri collaboratori/colleghi nel rispetto delle norme generali di utilizzo della rete Internet vigenti.

ART. 10 - LE APPLICAZIONI INFORMATICHE SPECIALISTICHE

10.1 Il RESPONSABILE del trattamento dei dati gestiti da una applicazione informatica specialistica è il Dirigente della STRUTTURA che gestisce il procedimento amministrativo cui l'applicazione fa riferimento.

10.2 Il rilascio delle credenziali ai soggetti interessati al trattamento dei dati contenuti negli applicativi specialistici viene autorizzato dal responsabile dell'applicativo stesso, su richiesta del Dirigente della STRUTTURA cui fa riferimento l'interessato.

10.3 La credenziale è di norma di tipo personale e può, caso per caso, rispondere a specifiche restrizioni di accesso, dipendendo dalle caratteristiche di riservatezza del sistema informativo cui si riferisce (presenza di dati aziendali, dati personali, dati sensibili, etc.)

10.4 Per l'utilizzo di applicazioni gestite su delega di Enti Esterni alla Amministrazione Comunale, le modalità di rilascio e gestione delle credenziali di accesso sono regolate su specifica richiesta motivata da parte del Dirigente richiedente, dalle apposite convenzioni stipulate tra la Amministrazione Comunale e ciascun Ente gestore (TITOLARE).

ART. 11 – USO DEI TELEFONI FISSI E DEI FAX

11.1 I telefoni "fissi" che l'Amministrazione mette a disposizione devono essere utilizzati in modo strettamente pertinente allo svolgimento dell'attività lavorativa o istituzionale, secondo un utilizzo appropriato, efficiente, corretto e razionale.

11.2 Solo in caso di necessità e urgenza, e qualora non possano utilizzare il proprio telefono cellulare, i dipendenti, amministratori e collaboratori dell'Ente possono utilizzare tali beni per motivi non attinenti l'attività lavorativa o istituzionale e, comunque, non in modo ripetuto o per periodi di tempo prolungati.

11.3 Nella categoria dei telefoni "fissi" di cui al comma 1 sono compresi anche i dispositivi "*voice over ip*" (ad esempio gli "*ip telefoni*").

11.4 Le disposizioni previste per i telefoni fissi si applicano anche ai fax che l'Amministrazione mette a disposizione.

ART. 12 – USO DEI DISPOSITIVI MOBILI

12.1 I dispositivi mobili (ad es. smartphone, tablet, notebook e simili), che l'Amministrazione comunale mette a disposizione devono essere utilizzati in modo strettamente pertinente allo svolgimento dell'attività lavorativa o istituzionale, secondo un utilizzo appropriato, efficiente, corretto e razionale.

12.2 I dispositivi mobili sono strumenti funzionali all'esecuzione della prestazione lavorativa. Sono utilizzabili senza necessità di procedura di autorizzazione ai sensi dell'art. 4, comma 2, della Legge n. 300/1970 e successive modificazioni, nel rispetto del Codice in materia di protezione di dati personali. Le procedure di autorizzazione di cui all'art. 4, comma 1, della

Legge n. 300/1970 e successive modificazioni, restano necessarie qualora le apparecchiature consentano di effettuare controlli indiretti e a distanza della prestazione lavorativa.

12.3 Il dipendente, l'amministratore e il collaboratore assegnatario di un dispositivo mobile dell'Amministrazione è responsabile del suo utilizzo e della sua custodia.

12.3 All'utilizzo dei dispositivi mobili dell'Amministrazione si applicano le medesime regole previste per l'utilizzo del telefono "fisso" di cui all'articolo precedente. L'eventuale uso promiscuo (anche per fini personali) del telefono cellulare dell'Amministrazione comunale è possibile, con addebito del costo delle comunicazioni e dei messaggi sullo stipendio, anteponendo l'apposito codice ai numeri di telefono del destinatario della comunicazione.

CAPO II

ISTRUZIONI E MISURE DI SICUREZZA PER IL TRATTAMENTO DEI DATI A CUI SI DEVONO ATTENERE GLI INCARICATI

ART. 13 – DEFINIZIONE DI TITOLARE, RESPONSABILE E INCARICATO DEL TRATTAMENTO DEI DATI PERSONALI

13.1 Il Codice in materia di protezione dei dati personali definisce i soggetti che effettuano il trattamento dei dati personali come segue:

"titolare" dei dati personali (art. 4, comma 1 lett. f) è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitariamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dai personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

"responsabile" (art. 4, comma 1 lett. g) è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

"incaricati" (art. 4, comma 1 lett. h), sono le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

13.2 Con Decreto del Sindaco n. 78 del 28 maggio 2004 sono stati individuati nei Dirigenti delle unità organizzative del Comune di Verona i "responsabili" del trattamento dei dati personali trattati dalle rispettive strutture, dando atto che ogni successiva variazione degli incarichi dirigenziali, comporterà conseguentemente anche l'automatica variazione dell'incarico di responsabile del trattamento dei dati, senza necessità di ulteriore e formale provvedimento.

ART. 14 – TRATTAMENTO DEI DATI EFFETTUATO CON STRUMENTI ELETTRONICI O COMUNQUE AUTOMATIZZATI

La classificazione dei sistemi di archiviazione e di trattamento dei dati costituenti il patrimonio informativo dell'Ente e le misure minime di sicurezza da adottare sono riassunte nella Tabella allegata al presente Regolamento.

I dati sono classificabili nelle seguenti tre tipologie:

DATI COMUNI

DATI PERSONALI

DATI SENSIBILI e/o GIUDIZIARI

É prevista, per ciascun trattamento, una politica di sicurezza che garantisca le misure minime cui attenersi.

PARTE I

TRATTAMENTO DEI DATI EFFETTUATO SU SISTEMI INFORMATICI AZIENDALI NON ACCESSIBILI DA ALTRI SISTEMI (SISTEMI ISOLATI).

1. MISURE DI SICUREZZA GENERALI

Per l'accesso ad ogni postazione di lavoro va prevista una credenziale (utenza e password) per l'accesso ai dati contenuti localmente.

PARTE II

TRATTAMENTO DEI DATI EFFETTUATO SU SISTEMI INFORMATICI AZIENDALI ACCESSIBILI IN RETE

1. CLASSIFICAZIONE

Ai fini della presente parte i sistemi informatici accessibili in rete impiegati nel trattamento dei dati sono distinti in:

a) sistemi accessibili con credenziali attraverso reti non disponibili al pubblico (reti private come la rete privata comunale);

b) sistemi accessibili mediante una rete di telecomunicazioni disponibile al pubblico (reti pubbliche come la rete internet).

CREDENZIALI E PROTEZIONE DEI SISTEMI INFORMATICI

Nel caso di trattamenti effettuati su sistemi di cui al punto 1 oltre a quanto previsto dalla Parte I, devono essere adottate le seguenti misure:

a) a ciascun INCARICATO DEL TRATTAMENTO è attribuita una credenziale personale per l'accesso alla rete;

a) le credenziali personali sono assegnate e gestite in modo che ne sia prevista la disattivazione in caso di perdita della qualità che consentiva l'accesso al sistema o di mancato utilizzo dei medesimi per un periodo superiore ai sei mesi;

b) i sistemi sono protetti contro il rischio di intrusione mediante idonei programmi antivirus, la cui efficacia ed aggiornamento sono verificati con cadenza almeno semestrale.

2. ACCESSO AI DATI SENSIBILI E/O GIUDIZIARI

Per il trattamento dei dati sensibili e/o giudiziari l'accesso per effettuare operazioni è determinato sulla base di autorizzazioni assegnate, singolarmente o per gruppi di lavoro, agli INCARICATI DEL TRATTAMENTO. Se il trattamento è effettuato su sistemi accessibili mediante una rete di telecomunicazioni disponibile al pubblico (come la rete internet), sono

oggetto di autorizzazione anche gli strumenti che possono essere utilizzati per l'interconnessione.

L'autorizzazione, se riferita agli strumenti, deve individuare i singoli sistemi attraverso i quali è possibile accedere per effettuare operazioni di trattamento.

Le autorizzazioni all'accesso sono rilasciate e revocate dal TITOLARE o dal RESPONSABILE. Periodicamente, e comunque almeno una volta l'anno, è verificata la sussistenza delle condizioni per la loro conservazione.

L'autorizzazione all'accesso deve essere limitata ai soli dati la cui conoscenza è indispensabile per lo svolgimento delle operazioni di trattamento.

La validità delle richieste di accesso è verificata prima di consentire l'accesso stesso.

I dati sono trattati con tecniche di cifratura (protocollo sicuro) o mediante l'utilizzazione di credenziali o di altri sistemi che, considerato il numero e la natura dei dati trattati, permettono di identificare gli interessati solo in caso di necessità.

I dati sono conservati, separatamente da ogni altro dato (comune o contenente dati personali) trattato per finalità che non richiedano il loro utilizzo. Al trattamento di tali dati si procede con le modalità di cui al comma precedente anche quando detti dati non sono contenuti in elenchi, registri o banche dati o non sono tenuti con l'ausilio di mezzi elettronici o comunque automatizzati.

ART. 15 – TRATTAMENTO DEI DATI CON STRUMENTI DIVERSI DA QUELLI ELETTRONICI O COMUNQUE AUTOMATIZZATI

15.1 Nel caso di trattamento di dati, effettuato con strumenti diversi da quelli elettronici o comunque automatizzati, sono osservate le seguenti modalità:

a) nel designare gli INCARICATI DEL TRATTAMENTO per iscritto e nell'impartire le istruzioni il TITOLARE o il RESPONSABILE devono prescrivere che gli incaricati abbiano accesso ai soli dati la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati;

b) gli atti e i documenti contenenti i dati devono essere conservati in archivi ad accesso selezionato definendo procedure di consegna e restituzione dei documenti.

15.2 Nel caso di trattamento di dati sensibili e/o giudiziari, oltre a quanto previsto nel comma 1, devono essere osservate le seguenti modalità:

a) gli atti e i documenti contenenti i dati sono conservati in luoghi chiusi, sale o contenitori muniti di serratura, accessibili al personale specificamente autorizzato;

b) l'accesso agli archivi deve essere controllato e devono essere identificati e registrati i soggetti che vi vengono ammessi dopo l'orario di chiusura degli archivi stessi.

ART. 16 – RESPONSABILITÀ IN CASO DI VIOLAZIONE DELLE ISTRUZIONI

16.1 Il mancato rispetto o la violazione delle regole contenute nel presente Regolamento e nella normativa italiana in materia di tutela dei dati, in particolare nel Codice sulla protezione dei dati personali emanato con D. Lgs. 196/2003, è perseguibile, nei confronti di dipendenti, amministratori e collaboratori, con provvedimenti disciplinari, nonché con le azioni civili e penali consentite.

16.2 Non sono ammesse segnalazioni di violazioni in forma anonima. Nei limiti previsti dalla normativa italiana in materia, l'Ente tutela il diritto alla privacy degli utenti che comunicano dette violazioni.

16.3 In caso di violazione delle istruzioni contenute nel presente Regolamento, si applicano le norme di legge, regolamento e contrattuali in vigore relative al procedimento disciplinare.

16.4 Oltre al presente Regolamento, l'Ente potrà mettere a disposizione degli utenti del materiale informativo utile alla corretta implementazione della policy dell'Ente in materia di trattamento dei dati, intendendo per policy la regolazione di una determinata funzione dell'Ente, contenente anche linee guida e suggerimenti per una migliore fruizione del servizio o dell'attività svolta.

ART. 17 – CONFIDENZIALITÀ DEI DATI PERSONALI TRATTATI

17.1 Gli incaricati sono tenuti a mantenere l'assoluta segretezza sulle informazioni di cui vengono a conoscenza nel corso delle operazioni di trattamento connesso ai procedimenti di competenza, evitando qualsiasi loro diffusione o comunicazione illegittima. Gli incaricati sono tenuti a non parlare di questioni riservate in aree pubbliche in modo tale che terzi possano udire la conversazione.

17.2 Gli incaricati del trattamento dei dati personali connesso all'attività di gestione documentale, realizzata attraverso il sistema di protocollo informatico dell'Ente, sono tenuti a mantenere l'assoluta segretezza sulle informazioni di cui vengono a conoscenza in una qualsiasi fase procedimentale in ragione della mansione e dell'utenza attribuita al programma di gestione del protocollo, evitando qualsiasi loro diffusione o comunicazione illegittima.

17.3 Gli incaricati del trattamento dei dati personali connesso agli adempimenti degli obblighi e dei compiti in materia di rapporto di lavoro e di impiego, sono tenuti a mantenere l'assoluta segretezza sulle informazioni di cui vengono a conoscenza in una qualsiasi fase procedimentale in ragione della mansione e dell'utenza attribuita al programma di gestione delle presenze del personale, evitando qualsiasi loro diffusione o comunicazione illegittima.

ART. 18 – PRECAUZIONI DA ADOTTARE NEL TRATTAMENTO DEI DATI CONTENUTI IN ARCHIVI E DOCUMENTI CARTACEI

18.1 Gli incaricati sono tenuti a custodire e controllare gli atti e i documenti contenenti dati personali, in modo da evitare che persone prive di autorizzazione possano accedere ai dati. I documenti contenenti dati personali devono essere conservati in archivi ad accesso controllato e con possibilità di chiusura. Tutta la documentazione e le pratiche trattate o da trattare devono essere riposte in armadi chiusi a chiave al termine della giornata lavorativa o comunque in caso di allontanamento prolungato.

18.2 I documenti contenenti dati sensibili o giudiziari devono essere classificati come tali e resi riconoscibili agli altri incaricati ed in particolare al personale preposto all'archiviazione. I documenti contenenti dati sensibili o giudiziari devono essere conservati in armadi chiusi.

18.3 Nel caso di richieste di dati personali tramite fax o posta elettronica, premesso che è preferibile la posta elettronica certificata, l'incaricato deve prestare attenzione a:

- verificare l'identità del richiedente (ad esempio nel caso in cui sia stato attribuito all'interessato un codice identificativo);
- digitare correttamente il numero di fax o l'indirizzo del destinatario e controllarne l'esattezza prima dell'invio;
- verificare che il documento venga spedito correttamente;
- attendere la stampa del rapporto di trasmissione verificando la corrispondenza tra il numero di pagine da inviare e quelle effettivamente inviate o la comunicazione dell'invio.

18.4 Nel caso di richieste di dati personali tramite telefono, l'incaricato deve prestare attenzione a:
- verificare l'identità del richiedente (ad esempio formulando una serie di quesiti a mezzo di intervista guidata oppure attribuendo all'interessato un codice identificativo che quest'ultimo gli comunicherà previamente ad ogni comunicazione impersonale);
- chiedere il numero di telefono dal quale è effettuata la chiamata;
- richiamare il numero fornito dal richiedente;
- controllare che il dato richiesto sia stato comunicato all'interessato fedelmente.
  Non comunque consentito comunicare dati sensibili e/o giudiziari tramite telefono.

18.5 Nel caso di acquisizione in formato digitale della documentazione cartacea tramite scanner, l'incaricato deve verificare che il contenuto del documento oggetto di scansione sia correttamente leggibile.

18.6 Gli incaricati preposti alla duplicazione di documentazione o alla sostituzione della documentazione cartacea con registrazione ottica devono prestare attenzione a non dimenticare l'originale del documento all'interno della macchina fotocopiatrice e/o dello scanner.

18.7 Gli incaricati preposti alla duplicazione di documentazione devono procedere alla distruzione controllata delle copie superflue, non più occorrenti o che presentino una forma non corretta. È necessario che evitino di gettare la documentazione nel cestino della carta straccia senza aver previamente provveduto a rendere inintelligibili i dati impressi sul supporto.

ART. 19 – PRECAUZIONI SPECIFICHE PER I RAPPORTI DI FRONT-OFFICE

19.1 Gli operatori di sportello sono tenuti a richiedere il rispetto dello spazio di cortesia. Ove necessario, devono invitare gli interessati a sostare dietro le linee tracciate sul pavimento o dietro le barriere che delimitano lo spazio di riservatezza.

19.2 Nei casi in cui sia necessario verificare l'identità dell'interessato per esigenze di garanzia di correttezza del dato da raccogliere, si suggerisce di richiedere ed ottenere un documento di riconoscimento.

19.3 L'incaricato deve prestare attenzione in sede di inserimento dei dati personali dell'interessato al fine di evitare errori di battitura che potrebbero creare problemi nel proseguo del processo.

ART. 20 – PRECAUZIONI DA ADOTTARE NEL TRATTAMENTO DEI DATI CONSEGUENTI ALL'ATTIVITÀ DI VIDEOSORVEGLIANZA

20.1 Gli incaricati del trattamento dei dati personali conseguenti all'attività di videosorveglianza e/o di rilevazione tramite videocitofono con possibile funzione di telecamera, possono prendere visione delle immagini registrate/rilevate, avendo cura di accedere ai soli dati personali strettamente necessari per il raggiungimento delle finalità perseguite, evitando - quando non indispensabili – immagini dettagliate, ingrandite o dettagli non rilevanti.

20.2 Gli incaricati del trattamento dei dati conseguenti all'attività di videosorveglianza e/o di rilevazione tramite videocitofono con possibile funzione di telecamera, devono vietare rigorosamente l'accesso ad altri soggetti, salvo si tratti di organi di polizia giudiziaria che devono accedervi per indagini di iniziativa o delegate dall'Autorità Giudiziaria in ordine a reati.

20.3 Gli incaricati del trattamento dei dati conseguenti all'attività di registrazione immagini tramite impianti di videosorveglianza, possono estrapolare filmati o fotogrammi nel rispetto dei tempi massimi di conservazione su richiesta degli organi di polizia giudiziaria che svolgono indagini d'iniziativa o delegate dall'Autorità Giudiziaria in ordine a reati o di pubblica sicurezza, avendo cura di limitare al numero di ore previste il periodo di conservazione delle immagini registrate.

ART. 21 – PRECAUZIONI DA ADOTTARE PER LA TUTELA DELLA SICUREZZA DEL SISTEMA INFORMATICO COMUNALE

21.1 Gli utenti, intendendo per essi qualsiasi persona che accede alle risorse informatiche comunali, devono fare riferimento, per qualsiasi dubbio riguardante la sicurezza informatica, esclusivamente al Responsabile della Direzione Informatica o persona da lui delegata. In nessun caso, l'utente comunica via e-mail, telefono, fax o altro mezzo di comunicazione non sicuro le proprie password o altre informazioni riservate inerenti al sistema informatico comunale senza l'autorizzazione del Responsabile della Direzione Informatica.

21.2 Si raccomanda agli utenti di prestare la massima attenzione nella stampa di documenti contenenti dati personali e di messaggi e-mail, soprattutto nel caso si utilizzino delle stampanti di gruppo o accessibili a più persone.

21.3 Qualsiasi supporto informatico mobile che permetta di portare dati all'esterno dell'Ente rappresenta un grave rischio e un punto di vulnerabilità per la sicurezza del sistema informatico comunale. Questi supporti portatili non dispongono infatti di adeguati sistemi di sicurezza. La replica su questi strumenti di qualsiasi dato personale potrebbe fornire a terzi informazioni riservate in caso di smarrimento, furto o sequestro dell'apparecchio.

21.4 Gli utenti sono tenuti a non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento, anche in caso di temporaneo allontanamento dalla postazione di lavoro. L'utente dovrà configurare il blocco reimpostato a tempo della propria postazione attraverso screensaver o in alternativa dovrà manualmente provvedere al blocco della postazione in caso di allontanamento anche temporaneo.

21.5 Gli utenti sono tenuti a conservare la segretezza della propria password e a sostituire in ogni caso la password ogni novanta giorni solari. La password dovrà essere composta da almeno 8 caratteri alfanumerici. Gli utenti sono tenuti a sostituire immediatamente la password, dandone comunicazione al Responsabile della Direzione Informatica, nel caso sospetti che la stessa abbia perso la segretezza e che qualcuno possa averla impropriamente utilizzata nella fase antecedente alla sua sostituzione.

21.6 L'utente è tenuto a seguire attentamente le disposizioni date dalla Direzione Informatica riguardo alla protezione da virus e da altri software pericolosi per il sistema informatico comunale. Nel caso in cui il software antivirus rilevi la presenza di un virus, l'utente deve seguire le indicazioni fornite dal programma. Qualora, a causa di un anomalo funzionamento del sistema, si sospetti la presenza di un virus che il software non sia stato in grado di riconoscere, si deve immediatamente: a) sospendere ogni elaborazione in corso senza spegnere il computer; b) segnalare l'accaduto alla Direzione Informatica.

Non è consentito l'utilizzo di supporti rimovibili di provenienza ignota. Ogni dispositivo magnetico di provenienza esterna all'Ente deve essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, deve essere consegnato all'amministratore di sistema.

ART. 22 – PRECAUZIONI DA ADOTTARE NELL'UTILIZZO DELLA POSTA ELETTRONICA IN ORDINE AL TRATTAMENTO DEI DATI

22.1 La confidenzialità della posta elettronica e della comunicazione attraverso il Web è limitata in quanto i messaggi, transitando nella rete pubblica di Internet, possono essere visionati da terzi non autorizzati. Il livello di confidenzialità di una e-mail, salvo non si tratta di posta elettronica certificata (PEC) si avvicina di più a quello di una cartolina piuttosto che a quello di una lettera. Per questa ragione è fatto divieto assoluto di comunicare informazioni classificate come riservate o dati sensibili attraverso l'e-mail o attraverso il Web se non esplicitamente autorizzati dal Dirigente dell'Unità organizzativa di appartenenza.
L'invio di comunicazioni elettroniche con informazioni personali riguardo al personale dell'Ente è sottoposta alla disciplina prevista dal Codice sulla protezione dei dati personali ed è previsto pertanto un diritto di accesso ai dati da parte degli interessati, anche qualora questi ultimi non risultino tra i destinatari della comunicazione elettronica.

22.2 L'attendibilità dell'identità del mittente è molto limitata nella comunicazione via e-mail. È relativamente facile, infatti, camuffare il mittente di una e-mail. Si richiede pertanto, ogni qual volta sia necessaria la certezza dell'identità del mittente, di verificarla con mezzi appropriati.
L'attendibilità della data ed ora esatta di invio di una e-mail è molto limitata. È relativamente facile, infatti, modificare questi dati. Si richiede pertanto, ogni qual volta sia necessaria la certezza della data e dell'ora del messaggio, di verificarle con i mezzi appropriati.

22.3 Gli utenti devono organizzare l'agenda del proprio programma di posta elettronica in modo che non vi possano essere degli errori nella selezione dei destinatari dei messaggi. È vietato l'uso di mass-mailing (spedizione di massa), pena la revoca dell'utenza mittente da parte della Direzione Informatica; per dare risalto ad eventi o iniziative comunali il corretto strumento pubblicitario interno è la intranet, quello esterno è il sito Internet del Comune di Verona.
Nell'invio di messaggi elettronici a molteplici destinatari interni all'Ente gli utenti sono invitati a non utilizzare la funzione Copia Carbone Nascosta (CCN, anche chiamata Blind Carbon Copy-Bcc), che permette di occultare ai destinatari la lista degli altri destinatari del messaggio. Quando si usa la funzione di inoltro, devono essere cancellate le informazioni non attinenti o direttamente rivolte al nuovo destinatario.

22.4 Gli utenti devono assicurarsi che nei loro messaggi elettronici non siano inserite inconsapevolmente informazioni su User e Password utilizzate per accedere ad altre

applicazioni. In particolare va usata la massima cautela nell'invio a mezzo posta elettronica di pagine internet che potrebbero contenere nell'indirizzo informazioni utili a risalire alla User/Password utilizzata.
Gli utenti sono invitati a nominare correttamente i nomi dei file allegati alle e-mail, specificando, nel caso si procedesse ad inviare documenti soggetti a modifiche e revisioni, la versione corrente del file con dei numeri progressivi.
È esplicitamente vietato l'invio di messaggi in risposta a richieste di adesione a programmi di catene di e-mail, indipendentemente dalle finalità presunte.
Gli utenti sono invitati a prestare attenzione nell'utilizzo della funzione "Rispondi" e "Rispondi a tutti" nel caso in cui il messaggio sia stato inviato ad un numero elevato di destinatari.

22.5 Gli utenti sono invitati a leggere quotidianamente la posta elettronica e a rispondere in tempi ragionevoli alle e-mail ricevute. Sono inoltre invitati a scrivere i propri messaggi di posta elettronica in plain text (7-bit ASCII) qualora non si siano previamente accertati che il destinatario è provvisto di un client di posta in grado di supportare la lettura di altri formati.
Gli utenti sono tenuti sempre ad accertarsi che gli eventuali allegati dei propri messaggi non eccedano la dimensione massima, stabilita dalla Direzione Informatica, indicato nelle istruzioni di utilizzo della posta. Qualora si riscontrasse la necessità di allegare un file di dimensioni superiori è buona norma che il mittente si assicuri previamente con il destinatario sulla possibilità di ricevere un messaggio di tali dimensioni.
Gli utenti sono invitati ad inviare allegati in formato standard, non proprietario senza l'utilizzo di macro. L'utilizzo di file con estensioni poco comuni potrebbe comportare la cancellazione del messaggio da parte del destinatario. Si faccia riferimento alla Direzione Informatica per dubbi in merito.
Si consiglia agli utenti di selezionare l'opzione che permette di inviare i messaggi immediatamente. La funzione che permette di metterli in coda per un successivo invio è caratterizzata da un'alta percentuale di casi di mancato o ritardato invio.
Si invitano gli utenti che hanno selezionato l'opzione di completamento automatico dell'indirizzo di prestare molta attenzione nella selezione dei destinatari.
Gli utenti devono periodicamente cancellare o organizzare in opportune cartelle la posta già letta. Una quantità troppo elevata di e-mail nella cartella predefinita di arrivo della nuova posta può compromettere sensibilmente la stabilità del programma di posta.

22.6 Gli utenti devono sempre indicare con chiarezza (nel campo oggetto), l'argomento del proprio messaggio. È possibile richiedere una ricevuta di corretto ricevimento della propria mail. A tale ricevuta va tuttavia assegnata una importanza relativa poiché talvolta la conferma della ricezione avviene ad opera del mail server centrale e non del destinatario ultimo del messaggio.
Gli utenti sono invitati a segnalare alla Direzione Informatica l'arrivo sistematico di messaggi non sollecitati (spam) da determinati indirizzi e-mail.
Gli utenti sono invitati ad utilizzare dei modelli di posta elettronica per i messaggi che vengono inviati frequentemente, e a prestare la massima attenzione nell'utilizzo delle funzioni avanzate di filtro che consentono di inoltrare automaticamente determinati messaggi in arrivo ad altri destinatari.

ART. 23 – PRECAUZIONI DA ADOTTARE NELLA NAVIGAZIONE IN INTERNET IN ORDINE AL TRATTAMENTO DEI DATI

23.1 È vietato connettersi autonomamente alla rete Internet con sistemi non approvati dalla Direzione Informatica, così come è vietato modificare le impostazioni del Web Browser stabilite dal Dirigente della Direzione Informatica.

23.2 Fatto salvo il divieto a navigare per fini diversi da quelli professionali, si suggerisce di evitare la navigazione in siti caratterizzati da scarsa serietà e attendibilità: si ricorda che è operativo un filtro automatico per la navigazione sicura.
Nel corso della navigazione l'utente è tenuto a leggere con attenzione qualsiasi finestra, pop up o avvertenza prima di proseguire nella navigazione e in particolare prima di accettare delle condizioni contrattuali o di aderire a delle iniziative online.
È fatto divieto assoluto di scaricare programmi o contenuti multimediali senza la previa autorizzazione del Dirigente della Direzione Informatica.

23.3 Gli utenti sono invitati a limitare il rilascio di dati personali durante la navigazione via Web. Qualsiasi informazione comunale prima di essere comunicata via Web deve essere autorizzata dal Dirigente responsabile.
Qualora il Dirigente autorizzi la comunicazione di dati sensibili o informazioni riservate via Web è necessario accertarsi che il sito sia ufficiale e conosciuto e che vi sia la protezione della comunicazione attraverso SSL. Ciò può essere verificato controllando che nel bordo inferiore destro del browser appaia il disegno di un piccolo lucchetto giallo chiuso.

23.4 Gli utenti sono invitati ad organizzare in modo ordinato la propria cartella dei siti Preferiti. Si consiglia agli utenti di salvare sul proprio spazio disco in locale i file .pdf e .doc scaricati dalla rete prima di aprirli.

ART. 24 – CUSTODIA E MANUTENZIONE DELLA POSTAZIONE DI LAVORO

24.1 Ogni utente è responsabile dell'integrità e del buon funzionamento della propria postazione di lavoro, delle periferiche ad essa collegate e del software utilizzato. A questo proposito si raccomanda di spegnere a fine lavoro la propria postazione (unità di base e dispositivi periferici, quali stampanti, scanner, masterizzatori) come misura per prevenire possibili surriscaldamenti o eventi accidentali negli uffici, a norma del Decreto legislativo 9 aprile 2008, n. 81 in materia di tutela della salute e della sicurezza nei luoghi di lavoro.
Non è permesso aggiungere, disinstallare o comunque modificare il software fornito o la configurazione della propria postazione; la violazione di tale regola non consente alla Direzione Informatica di garantire il corretto funzionamento della strumentazione informatica in dotazione agli uffici.
In tutti i casi in cui si rende necessario installare nuove postazioni di lavoro o dotare quelle già in essere di nuove componenti o programmi, la richiesta va sottoposta direttamente alla Direzione Informatica, che ne valuterà la fattibilità, demandandone l'implementazione, se del caso, a risorse interne o mediante acquisizione/sviluppo di applicativi con società terze parti.

CAPO III

DISPOSIZIONI FINALI

ART. 25 – PRIORITÀ DELLE MISURE TECNICHE DI PROTEZIONE

25.1 L'Amministrazione si impegna ad attuare, in primo luogo, misure tecniche di protezione contro l'utilizzazione abusiva e i guasti tecnici (ad es. bloccando la navigazione in Internet nelle ore notturne e fino all'inizio dell'orario si servizio, filtrando taluni siti, etc.). Tali misure sono regolarmente adeguate allo stato più recente della tecnica. L'adeguamento avviene anche dopo ogni problema tecnico.

ART. 26 – COMPITI DI SORVEGLIANZA

26.1 I responsabili di ciascuna Unità Organizzativa hanno il compito di sorvegliare il corretto rispetto delle modalità di utilizzo delle risorse informatiche in dotazione ai dipendenti, nonché di disporre eventuali ulteriori direttive giudicate necessarie nell'ambito di particolari specificità o responsabilità.

ART. 27 – GRADUALITÀ DEI CONTROLLI

27.1 Qualsiasi forma di controllo venga effettuata, deve essere strettamente necessaria per il Datore di lavoro in relazione a scopi determinati e per il perseguimento di finalità organizzative, produttive e di sicurezza.

27.2 Nell'eventualità di anomalie riscontrate nell'utilizzo delle risorse informatiche messe a disposizione dall'Amministrazione comunale oppure in caso di richieste di verifica da parte dei responsabili delle varie strutture comunali per presunte anomalie nell'utilizzo di tali risorse da parte del personale ad essi assegnato, o dei collaboratori o amministratori che ne fanno uso, il Dirigente della Direzione Informatica, o personale incaricato dallo stesso, comunica la situazione riscontrata, senza indicazione di nominativi, al Dirigente responsabile della struttura nella quale è stata rilevata l'anomalia o al Dirigente che ha richiesto la verifica. Quest'ultimo provvede, a sua volta, ad inviare un avviso generalizzato diretto a tutti i dipendenti appartenenti alla struttura nella quale la situazione è stata riscontrata, nel quale evidenzia l'utilizzo irregolare degli strumenti dell'Amministrazione e invita gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

27.3 Se l'avviso generalizzato di cui al comma 2 non produce effetto e l'anomalia rilevata persiste, il Dirigente della Direzione Informatica, o personale incaricato dallo stesso, procede ad un controllo su base individuale e nominativa, a seguito del quale il medesimo Dirigente effettua una seconda segnalazione al Dirigente della struttura presso la quale è inserito il dipendente o il collaboratore interessato dalle verifiche o opera l'Amministratore. Il Dirigente di tale struttura, effettuate le necessarie verifiche, attiverà il procedimento disciplinare nei confronti del dipendente, secondo la normativa vigente per il personale o per l'area dirigenza del comparto Regioni ed Autonomie Locali. Per quanto riguarda i collaboratori verranno adottate le sanzioni previste dai relativi contratti, ivi compresa la disattivazione dell'utenza. Qualora invece l'utente autorizzato ricopra una carica istituzionale presso l'Ente, dovranno essere avvisati il sindaco, il presidente del consiglio comunale o del consiglio di circoscrizione, a seconda della carica rivestita, nonché il dirigente della struttura di riferimento per i provvedimenti interdittivi del caso,

ivi compresa l'eventuale disattivazione dell'utenza. L'Amministrazione è tenuta alla riservatezza in tutte le fasi di accertamento dei fatti.

27.4 Nell'eventualità di anomalie riscontrate nell'utilizzo degli strumenti di comunicazione telefonica, fissa, mobile e palmare, messi a disposizione dall'Amministrazione comunale oppure in caso di richieste di verifica da parte dei responsabili delle varie strutture comunali per presunte anomalie nell'utilizzo di tali strumenti da parte del personale ad essi assegnato, il Dirigente della Direzione Economato Gestione Contratti Utenze, o personale incaricato dallo stesso, chiede l'invio della documentazione relativa al traffico telefonico al gestore del servizio, tramite richiesta a firma del coordinatore comunale privacy corrispondente al Dirigente della Direzione Affari Generali. A seguito ricevimento della documentazione comunica la situazione riscontrata, senza indicazione di nominativi, al Dirigente responsabile della struttura nella quale è stata rilevata l'anomalia o al Dirigente che ha richiesto la verifica. Quest'ultimo provvede, a sua volta, ad inviare un avviso diretto a tutti i dipendenti appartenenti alla sua struttura, o a coloro che sono autorizzati ad utilizzare la specifica utenza, nel quale evidenzia l'utilizzo irregolare degli strumenti dell'Amministrazione e invita i dipendenti e i collaboratori medesimi ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

27.5 Se l'avviso generalizzato di cui al comma 4 non produce effetto e l'anomalia rilevata persiste, il Dirigente della Direzione Economato Gestione Contratti Utenze, o personale incaricato dallo stesso, procede ad un nuovo controllo, a seguito del quale il medesimo Dirigente effettua una seconda segnalazione al Dirigente della struttura presso la quale è inserito il dipendente o il collaboratore od opera l'amministratore interessato dalle verifiche. Il Dirigente di tale struttura, effettuate le necessarie verifiche, attiverà il procedimento disciplinare nei confronti del dipendente, secondo la normativa vigente per il personale o per l'area dirigenza del comparto Regioni ed Autonomie Locali. Per quanto riguarda i collaboratori verranno adottate le sanzioni previste dai relativi contratti, ivi compresa la disattivazione dell'utenza. Qualora invece l'utente autorizzato ricopra una carica istituzionale presso l'Ente, dovranno essere avvisati il sindaco, il presidente del consiglio comunale o del consiglio di circoscrizione, a seconda della carica rivestita, nonché il dirigente della struttura di riferimento per i provvedimenti sanzionatori del caso, ivi compresa l'eventuale disattivazione dell'utenza. L'Amministrazione è tenuta alla riservatezza in tutte le fasi di accertamento dei fatti.

27.6 Responsabile della rilevazione delle anomalie e delle verifiche tecniche di cui ai precedenti commi 2 e 3, è il Dirigente della Direzione Informatica; mentre Responsabile della rilevazione delle anomalie e delle verifiche tecniche di cui ai precedenti commi 4 e 5 è il Dirigente della Direzione Economato Gestione Contratti Utenze. Responsabili dei successivi e consequenziali provvedimenti sono il Dirigente della struttura interessata ed il Direttore dell'Area Risorse Umane e Strumentali, in conformità alle disposizioni di legge e dei CCNL vigenti.

27.7 L'Amministrazione, nel rispetto del principio di protezione dei dati personali e del divieto di controllo a distanza dei dipendenti, procede, in caso di anomalie, alla conservazione delle "*registrazioni a giornale*" (*log file*) relative all'utilizzazione di internet e della Posta Elettronica e dei tabulati delle telefonate e dei fax, per il tempo strettamente necessario alla soluzione delle suddette anomalie.

ART. 28 – DISTINZIONE TRA E-MAIL PRIVATE ED E-MAIL PROFESSIONALI

28.1 Le e-mail private o riservate è opportuno che siano contrassegnate con la menzione "Privato" o "Riservato" all'inizio dell'Oggetto. Fermi restando i limiti generali di accesso da parte del Datore di lavoro alla posta elettronica messa a disposizione dell'intestatario della casella, all'Amministrazione non è consentito prendere visione delle e-mail che recano la menzione "Privato" o "Riservato". Resta fermo quanto indicato all'art. 8 (*Il Sistema di Posta Elettronica)* del presente Regolamento.

28.2 In caso di controllo su base individuale e nominativa, allorché non ci sia distinzione fra Posta Elettronica privata e professionale e la natura privata di un messaggio non sia riconoscibile, l'Amministrazione presuppone che si tratti di Posta Elettronica professionale. Alla presenza di fondati dubbi circa la natura professionale di un messaggio la questione deve essere chiarita con l'intestatario della casella.

ART. 29 – OBBLIGATORIETÀ OSSERVANZA DISPOSIZIONI E SANZIONI

29.1 È fatto obbligo a tutti i dipendenti, amministratori e collaboratori dell'Ente di osservare le disposizioni portate a conoscenza con il presente Regolamento.

29.2 Il mancato rispetto o la violazione delle regole contenute nel presente Regolamento è perseguibile con tutte le azioni civili e penali previste dalla legge, nonché con i provvedimenti disciplinari, in conformità a quanto previsto dalle disposizioni di legge, regolamento e contrattuali vigenti per il personale o per l'area dirigenza del comparto Regioni ed Autonomie Locali.

ART. 30 – DISPOSIZIONI ULTERIORI

30.1 I dati personali inerenti i dipendenti non possono essere portati a conoscenza di terzi non autorizzati. I colleghi di lavoro della persona interessata sono considerati terzi.

30.2 Le "*registrazioni a giornale*" (*log file*) relative all'utilizzazione di Internet vengono sovra scritte automaticamente o comunque distrutte in modo che siano conservate per un periodo non superiore a tre mesi .

30.3 L'Amministrazione, nell'ambito di procedimenti disciplinari e/o di procedimenti penali di cui all'art. 27 del presente Regolamento e nel rispetto del principio di protezione dei dati personali e del divieto di controllo a distanza dei dipendenti, procede alla conservazione delle "*registrazioni a giornale*" (*log file*) relative all'utilizzazione di internet e/o della Posta Elettronica e/o dei tabulati delle telefonate e/o dei fax, fino alla conclusione dei relativi procedimenti.

30.4 Le e-mail inviate e ricevute dai Rappresentanti Sindacali aventi titolo, per la parte relativa all'attività sindacale, godono della tutela accordata alle e-mail di tipo "Privato" o "Riservato" di cui all'art. 28, comma 1.

30.5 Il presente Regolamento potrà essere soggetto a revisioni periodiche, anche su eventuale proposta delle organizzazioni di rappresentanza dei lavoratori o dei singoli dipendenti.

30.6 Il presente Regolamento deve essere portato a conoscenza di tutti i dipendenti, dei collaboratori e di eventuali intestatari, diversi dai dipendenti e dai collaboratori, di caselle di Posta Elettronica e/o abilitati ad accedere a internet, utilizzando quale strumento di comunicazione interna la intranet aziendale.

ART. 31 – ESERCIZIO DEI DIRITTI EX ART. 7 D.LGS. 196/2003

31.1 I dipendenti, gli amministratori e i collaboratori possono esercitare i diritti previsti dal D.Lgs. 196/2003 rivolgendosi al Titolare del trattamento: Comune di Verona con sede in Verona - Piazza Brà 1 o rivolgendosi ai Responsabili del trattamento (ex art. 29 del D.Lgs. 196/2003) individuati: nel Dirigente della Direzione Informatica con sede in Verona - Via degli Alpini 11 per quanto riguarda le segnalazioni di cui ai commi 2 e 3 del precedente art. 27; nel Dirigente della Direzione Economato Gestione Contratti Utenze , con sede in Verona - Via Campo Marzo 8 per quanto riguarda le segnalazioni di cui ai commi 4 e 5 del precedente art. 27; nel Dirigente di struttura per tutto ciò che attiene alla gestione del rapporto di lavoro; nel Direttore dell'Area Risorse Umane e Strumentali con sede in Verona - Piazza Brà 1 per tutti gli atti di propria competenza previsti dalle disposizioni contrattuali e legislative vigenti.

ART. 32 – DISPOSIZIONI DI RINVIO

32.1 Si fa riserva di adottare successive eventuali integrazioni o correzioni alle disposizioni del presente regolamento, in relazione all'entrata in vigore di sopravvenute normative ed all'evolversi della tecnologia.

CLASSIFICAZIONE DEI SISTEMI DI ARCHIVIAZIONE E DI TRATTAMENTO DEI DATI E MISURE MINIME DI SICUREZZA DA ADOTTARE AI SENSI DEL D. LGS. 196/2003

TIPO DI SISTEMA	MISURE MINIME DI SICUREZZA			
	DATI COMUNI	DATI PERSONALI	DATI SENSIBILI e/o GIUDIZIARI	AGGIORNAMENTO
Sistema Informatico isolato (modalità stand alone)	Password	Password	Password	Trimestrale
Sistema accessibile da utenze attraverso rete comunale privata (rete privata comunale)	• Password • Credenziale per ciascun gruppo di incaricati del trattamento • Antivirus	• Password • Credenziale personale per ciascun incaricato del trattamento • Antivirus	• Password • Credenziale per ciascun incaricato del trattamento • Antivirus • Autorizzazioni di accesso singole o per gruppi di lavoro da rilasciare agli incaricati del trattamento	Per quanto riguarda le password, v. art. 21.5 Semestrale
Sistema accessibile da utenze mediante una rete di telecomunicazioni pubblica (come la rete internet)	• Password • Credenziale per ciascun gruppo di incaricati del trattamento • Antivirus	• Password • Credenziale personale per ciascun incaricato del trattamento • Antivirus	• Password • Credenziale (utenza) per ciascun utente o incaricato del trattamento • Antivirus • Documento programmatico sulla sicurezza	Semestrale Annuale
Archivi cartacei	• Accesso selezionato • Credenziale personale per ciascun incaricato del trattamento	• Accesso selezionato • Credenziale personale per ciascun incaricato del trattamento	• Accesso selezionato • Procedure di consegna e restituzione dei documenti • A disposizione degli incaricati, contenitori muniti di serratura • Controllo e registrazione dell'accesso agli archivi dopo l'orario di chiusura	