COPIA

DELIBERAZIONE 18
IN DATA 23.05.2018
PROTOCOLLO N° 415

CONSIGLIO DI BACINO VENETO ORIENTALE

ESTRATTO DEL VERBALE DEL COMITATO ISTITUZIONALE

OGGETTO: Regolamento per l'utilizzo dei sistemi informatici. **Approvazione.**

L'anno duemiladiciotto addì 23 del mese di Maggio alle ore 15.00 in continuazione, in CONEGLIANO nella sede del Consiglio di Bacino "Veneto Orientale", a seguito di inviti scritti diramati dal Presidente con lettera prot. n.412 in data 22.05.2018 si è riunito il COMITATO ISTITUZIONALE con l'intervento dei Sigg.:

N°	COGNOME E NOME	PRESENTI	ASSENTI
1	FABIO VETTORI – Presidente	X	
2	GILBERTO DANIEL– Componente	X	
3	FLORIANO ZAMBON – Componente	X	

Partecipa l'infrascritto Direttore Dott. Agostino Battaglia

Assume la Presidenza l'Ing. Fabio Vettori, il quale constatata la legalità della seduta la dichiara aperta, invitando il Comitato Istituzionale a deliberare sull'oggetto.

DELIBERAZIONE N. 18

DEL 23.05.2018
PROT. 415

OGGETTO: REGOLAMENTO PER L'UTILIZZO DEI SISTEMI INFORMATICI.
APPROVAZIONE.

IL COMITATO ISTITUZIONALE

PREMESSO:

- che è necessario approvare il Regolamento per l'utilizzo dei sistemi informatici da parte dei dipendenti e collaboratori di questo Consiglio di Bacino;

VISTO l'allegato Regolamento, la cui finalità è quella di promuovere in tutto il personale dell'Ente una corretta "cultura informatica" affinché l'utilizzo degli strumenti informatici e telematici forniti da questo Ente sia conforme alle finalità istituzionali e nel pieno rispetto delle norme di legge in vigore;

VISTA la Legge 20.05.1970 n.300;

VISTO li Regolamento Europeo n.679/16;

VISTE le linee guida del Garante per posta elettronica e internet pubblicate nella Gazzetta Ufficiale della Repubblica Italiana n.58 del 10.03.2007;

VISTO l'art.23 del D.Lgs. n.151/2015;

VISTA la L.R. n. 17 del 27/04/2012;

VISTO la Convenzione del Consiglio di Bacino "Veneto Orientale";

VISTO l'allegato parere favorevole del Vice Direttore in ordine alla regolarità tecnica e contabile espresso ai sensi dell'art. 49 del D. Lgs. n. 267 del 18.08.2000;

RITENUTO di doversi dichiarare la presente deliberazione con separata votazione immediatamente eseguibile;

CON voti unanimi espressi a termini di legge;

DELIBERA

- di dare atto che le premesse costituiscono parte integrante e sostanziale della presente deliberazione;
- di approvare il Regolamento per l'utilizzo dei sistemi informatici, allegato al presente atto;
- di disporre la trasmissione del presente Regolamento a tutti i dipendenti del Consiglio di Bacino "Veneto Orientale" mediante posta elettronica;

- di disporre altresì l'affissione del Regolamento all'albo di questo Consiglio di Bacino;
- di dare atto che il presente provvedimento rientra nella competenza del Comitato Istituzionale ai sensi della Convenzione del Consiglio di Bacino;
- di dare atto che sono stati espressi i pareri in ordine alla regolarità tecnica e contabile ai sensi dell'art. 49 del D.Lgs. n. 267 del 18.08.2000;
- di dichiarare la presente deliberazione immediatamente eseguibile ai sensi del 4° comma dell'art. 134 del D.Lgs. n. 267 del 18.08.2000;
- di pubblicare il presente provvedimento all'Albo ai sensi dell'art. 125 del D. Lgs. n. 267 del 18.08.2000;

VISTO
IL DIRETTORE
F.to Dott. Agostino Battaglia

REGOLAMENTO
PER L'UTILIZZO DEI
SISTEMI INFORMATICI

Indice

Changelog

Versione	Data	Cambiamenti effettuati dall'ultima versione

Premessa

Il presente Regolamento intende fornire ai dipendenti e collaboratori, denominati anche incaricati o utenti, dell'Amministrazione del CONSIGLIO DI BACINO VENETO ORIENTALE (di seguito più semplicemente "Ente") le indicazioni per una corretta e adeguata gestione delle informazioni aziendali, in particolare attraverso l'uso di sistemi, applicazioni e strumenti informatici dell'Ente.
Ogni dipendente e collaboratore è tenuto a rispettare il Regolamento, che è reso disponibile tramite le modalità specificate al successivo punto 16.
Si specifica che tutti gli strumenti utilizzati dal lavoratore, intesi con ciò i PC, notebook, risorse, e-mail ed altri strumenti con relativi software e applicativi (di seguito più semplicemente "Strumenti"), sono messi a disposizione dall'Ente per rendere la prestazione lavorativa. Gli Strumenti, nonché le relative reti dell'Ente a cui è possibile accedere tramite gli stessi, sono domicilio informatico dell'Ente.
I dati personali e le altre informazioni dell'Utente che sono registrati negli Strumenti o che si possono eventualmente raccogliere tramite il loro uso, sono utilizzati per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale. Per tutela del patrimonio aziendale si intende altresì la sicurezza informatica e la tutela del sistema informatico aziendale. Tali informazioni sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, visto che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Regolamento Europeo 679/16 "General Data Protection".
Viene, infine, precisato che non sono installati o configurati sui sistemi informatici in uso agli utenti apparati hardware o strumenti software aventi come scopo il controllo a distanza dell'attività dei lavoratori, fatti salvi quelli elencati al successivo punto 11 necessari per l'assistenza remota agli Utenti.

1 - Oggetto e finalità

Il presente Regolamento è redatto:

- alla luce della Legge 20.5.1970, n. 300, recante "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento";
- in attuazione del Regolamento Europeo 679/16 "General Data Protection" (d'ora in avanti Reg. 679/16 o GDPR);
- ai sensi delle "Linee guida del Garante per posta elettronica e internet" in Gazzetta Ufficiale n. 58 del 10 marzo 2007;
- alla luce dell'articolo 23 del D.Lgs. n. 151/2015 (c.d. Jobs Act) che modifica e rimodula la fattispecie integrante il divieto dei controlli a distanza, nella consapevolezza di dover tener conto, nell'attuale contesto produttivo, oltre agli impianti audiovisivi, anche degli altri strumenti *«dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori»* e di quelli *«utilizzati dal lavoratore per rendere la prestazione lavorativa»*.

La finalità è quella di promuovere in tutto il personale aziendale una corretta "cultura informatica" affinché l'utilizzo degli Strumenti informatici e telematici forniti dall'Ente, quali la posta elettronica, internet e i personal computer con i relativi software, sia conforme alle finalità aziendali e nel pieno rispetto della legge. Si vuole fornire a tutto il personale le indicazioni necessarie con l'obiettivo principale di evitare il verificarsi di qualsiasi abuso o uso non conforme, muovendo dalla convinzione che la prevenzione dei problemi sia preferibile rispetto alla loro successiva correzione.

1 Principi generali e di riservatezza nelle comunicazioni

1.1. I principi che sono a fondamento del presente Regolamento sono gli stessi espressi nel GDPR, e, precisamente:

a) **il principio di necessità**, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (art. 5 e 6 del Reg. 679/16);

b) **il principio di correttezza**, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori. Le tecnologie dell'informazione (in modo più marcato rispetto ad apparecchiature tradizionali) permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa. Ciò, all'insaputa o senza la piena consapevolezza dei lavoratori, considerate anche le potenziali applicazioni di regola non adeguatamente conosciute dagli interessati;

c) **i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime** (art.5 commi 1 e 2), osservando il principio di pertinenza e non eccedenza. Il datore di lavoro deve trattare i dati "nella misura meno invasiva possibile"; le attività di monitoraggio devono essere svolte solo da soggetti preposti ed essere "mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza".

1.2. È riconosciuto al datore di lavoro di potere svolgere attività di monitoraggio, che nella fattispecie saranno svolte solo dall'Amministratore di Sistema o dal personale delegato dall'Amministratore di Sistema, sempre nel rispetto della succitata normativa.

1.3. Il dipendente si attiene alle seguenti regole di trattamento:

a) È vietato comunicare a soggetti non specificatamente autorizzati i dati personali comuni, sensibili, giudiziari, sanitari o altri dati, elementi e informazioni aziendali dei quali il dipendente / collaboratore viene a conoscenza nell'esercizio delle proprie funzioni e mansioni all'interno dell'Ente. In caso di dubbio, è necessario accertarsi che il soggetto cui devono essere comunicati i dati sia o meno autorizzato a riceverli, mediante richiesta preventiva al proprio Responsabile di area/funzione.

b) È vietata l'estrazione di originali e/o copie cartacee ed informatiche per uso personale di documenti, manuali, fascicoli, lettere, data base e quant'altro.

c) È vietato lasciare incustoditi documenti, lettere, fascicoli, appunti e quant'altro possa contenere dati personali e/o informazioni aziendali quando il dipendente/collaboratore si allontana dalla postazione di lavoro. È vietato lasciare sulla postazione di lavoro (scrivania, bancone ecc.) materiali che non siano inerenti la pratica che si sta trattando in quel momento. Ciò vale soprattutto nel caso di lavoratori con mansioni di front office e di ricezione di Clienti / Fornitori o colleghi di lavoro.

d) Per le riunioni e gli incontri con Clienti, Fornitori, Consulenti e Collaboratori dell'Ente è necessario utilizzare le apposite Sale dedicate, se presenti.

2 - Tutela del lavoratore

2.1 Alla luce dell'art. 4, comma 1, L.n. 300/1970, la regolamentazione della materia indicata nell'art. 1 del presente Regolamento, non è finalizzata all'esercizio di un controllo a distanza dei lavoratori da parte del datore di lavoro, ma solo a permettere a quest'ultimo di utilizzare sistemi informativi per fare fronte ad esigenze produttive od organizzative e di sicurezza nel trattamento dei dati personali.

2.2 È garantito al singolo lavoratore il controllo sui propri dati personali secondo quanto previsto dagli articoli 15-16-17-18-20-21-78 del Reg. 679/16.

3 Campo di applicazione

3.1 Il presente regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o di livello, nonché a tutti i collaboratori dell'Ente a prescindere dal rapporto contrattuale con la stessa intrattenuto.

3.2 Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "Utente" deve intendersi ogni dipendente e collaboratore in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata come "Incaricato del trattamento".

4 Gestione, assegnazione e revoca delle credenziali di accesso

4.1 Le credenziali di autenticazione per l'accesso alle risorse informatiche vengono assegnate dai Servizi Informatici o da apposito incaricato, previa richiesta del Responsabile dell'ufficio/servizio nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente. Nel caso di collaboratori esterni la richiesta dovrà essere inoltrata direttamente dal Responsabile dell'Ufficio/Servizio con il quale il collaboratore si coordina nell'espletamento del proprio incarico. La richiesta di attivazione delle credenziali dovrà essere completa di generalità dell'utente ed elenco dei sistemi informativi per i quali deve essere abilitato l'accesso. Ogni successiva variazione delle abilitazioni di accesso ai sistemi informativi dovrà essere richiesta formalmente dal servizio Sistemi informativi o da apposito incaricato dal Responsabile di riferimento.

4.2 Le credenziali di autenticazioni consistono in un codice per l'identificazione dell'utente (altresì nominati username, nome utente o user id), assegnato dall'Ufficio Sistemi Informativi o da apposito incaricato, ed una relativa password. La password è personale e riservata e dovrà essere conservata e custodita dall'incaricato con la massima diligenza e non divulgata.

4.3 La password deve essere di adeguata robustezza: deve essere composta da almeno 8 caratteri, formata da lettere maiuscole e minuscole e/o numeri. Non deve contenere riferimenti agevolmente riconducibili all'utente (username, nomi o date relative alla persona o ad un famigliare).

4.4 È necessario procedere alla modifica della password a cura dell'utente al primo accesso e, successivamente, almeno ogni sei mesi. Nel caso in cui l'utente svolga mansioni che, in astratto, possano comportare il trattamento di dati personali sensibili, è obbligatorio il cambio password almeno ogni tre mesi.

4.5 Nel caso di cessazione del rapporto di lavoro con il dipendente/collaboratore, il Responsabile dell'Ufficio/area di riferimento dovrà comunicare formalmente e preventivamente all'Ufficio Sistemi Informativi o all'apposito incaricato la data effettiva a partire dalla quale le credenziali saranno disabilitate.

5 - Utilizzo della rete dell'Ente

5.1 Per l'accesso alle risorse informatiche dell'Ente attraverso la rete locale, ciascun utente deve essere in possesso di credenziali di autenticazione secondo il precedente art. 4.

5.2 È assolutamente proibito accedere alla rete e nei sistemi informativi utilizzando credenziali di altre persone.

5.3 L'accesso alla rete garantisce all'utente la disponibilità di condivisioni di rete (cartelle su server) nelle quali vanno inseriti e salvati i files di lavoro, organizzati per area/ufficio o per diversi criteri o per obiettivi specifici di lavoro. Tutte le cartelle di rete, siano esse condivise o personali, possono ospitare esclusivamente contenuti professionali. Pertanto è vietato il

salvataggio sui server dell'Ente, ovvero sugli Strumenti, di documenti non inerenti l'attività lavorativa, quali a titolo esemplificativo documenti, fotografie, video, musica, pratiche personali, sms, mail personali, film e quant'altro. Ogni materiale personale rilevato dall'Amministratore di Sistema o dall'Ufficio Sistemi Informativi o da apposito incaricato a seguito di interventi di sicurezza informatica ovvero di manutenzione/aggiornamento su server ed anche su Strumenti viene rimosso secondo le regole previste nel successivo punto 12 del presente Regolamento, ferma ogni ulteriore responsabilità civile, penale e disciplinare. Tutte le risorse di memorizzazione, diverse da quelle citate al punto precedente, non sono sottoposte al controllo regolare degli Amministratori di Sistema e non sono oggetto di backup periodici. A titolo di esempio e non esaustivo si citano: il disco C o altri dischi locali dei singoli PC, la cartella "Documenti" o "Desktop" dell'utente, gli eventuali dispositivi di memorizzazione locali o di disponibilità personale come Hard disk portatili o NAS ad uso esclusivo. Tutte queste aree di memorizzazione non devono ospitare dati di interesse aziendale, poiché non sono garantite la sicurezza e la protezione contro la eventuale perdita di dati. Pertanto la responsabilità dei salvataggi dei dati ivi contenuti è a carico del singolo utente.

5.4 Senza il consenso del Titolare, è vietato trasferire documenti elettronici dai sistemi informativi e Strumenti dell'Ente a device esterni (hard disk, chiavette, CD, DVD e altri supporti).

5.5 Senza il consenso dell'Ufficio Sistemi Informativi o di apposito incaricato è vietato salvare documenti elettronici dell'Ente (ad esempio pervenuti via mail o salvati sul Server o sullo Strumento in dotazione) su repository esterne (quali ad esempio Dropbox, GoogleDrive, OneDrive, ecc.) ovvero inviandoli a terzi via posta elettronica o con altri sistemi.

5.6 Con regolare periodicità (almeno una volta al semestre), ciascun utente provvede alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

5.7 L'Ente mette a disposizione dei propri utenti la possibilità di accedere alle proprie risorse informatiche anche dall'esterno dei confini aziendali, mediante rete VPN (Virtual Private Network), un canale privato e criptato verso la rete interna. L'accesso mediante VPN viene concesso a consulenti, professionisti, tecnici e fornitori che nell'ambito di un rapporto contrattuale con L'Ente necessitino di accedere a determinate risorse informatiche. Viene concesso, altresì, a dipendenti e funzionari dell'Ente che necessitino di svolgere compiti specifici, pur non essendo presenti in sede. Le richieste di abilitazione all'accesso mediante VPN dovranno seguire le prescrizioni del punto 4.

5.8 I Servizi Informatici o l'apposito incaricato si riservano la facoltà di negare o interrompere l'accesso alla rete mediante dispositivi non adeguatamente protetti e/o aggiornati, che possano costituire una concreta minaccia per la sicurezza informatica aziendale.

I log relativi all'uso del File System, nonché i file salvati o trattati su Server o Strumenti, sono registrati e possono essere oggetto di controllo da parte del Titolare del trattamento, attraverso i Servizi Informatici o apposito incaricato, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale.
I controlli possono avvenire secondo le disposizioni previste al successivo punto 12 del presente Regolamento.
Le informazioni così raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 679/16 "General Data Protection".

6 Utilizzo degli Strumenti elettronici (PC, notebook e altri strumenti con relativi software e applicativi)

6.1 Il dipendente/collaboratore è consapevole che gli Strumenti forniti sono di proprietà d'Ente e devono essere utilizzati esclusivamente per rendere la prestazione lavorativa Ognuno è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione. Ogni utilizzo non inerente all'attività lavorativa è vietato in quanto può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Ciascun dipendente /collaboratore si deve quindi attenere alle seguenti regole di utilizzo degli Strumenti.

6.2 L'accesso agli Strumenti aziendali è protetto da password; per l'accesso devono essere utilizzati Username e password assegnate dall'Ufficio Sistemi Informativi o dall'apposito incaricato (cfr. 4). A tal proposito si rammenta che essi sono strettamente personali e l'utente è tenuto a conservarli nella massima segretezza.

6.3 Il Personal Computer, notebook, tablet ed ogni altro hardware deve essere custodito con cura da parte degli assegnatari evitando ogni possibile forma di danneggiamento e segnalando tempestivamente al personale dell'Ufficio Sistemi Informativi Informativi o all'apposito incaricato ogni malfunzionamento e/o danneggiamento. Non è consentita l'attivazione della password d'accensione (BIOS), senza preventiva autorizzazione da parte dell'Amministratore di Sistema.

6.4 Non è consentito all'utente modificare le caratteristiche hardware e software impostate sugli Strumenti assegnati, salvo preventiva autorizzazione da parte del personale dell'Amministratore di Sistema Informativi o dell'apposito incaricato.

6.5 L'utente è tenuto a scollegarsi dal sistema, o bloccare l'accesso, ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro (PC) o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima: lasciare un PC incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. L'eventuale blocco temporaneo del pc può essere predisposto mediante l'attivazione di "screen saver" con password.

6.6 Le informazioni archiviate sul PC locale devono essere esclusivamente quelle necessarie all'attività lavorativa assegnata.

6.7 Costituisce buona regola la pulizia periodica degli archivi memorizzati sul proprio PC, con cancellazione dei file obsoleti o non più utili.

6.8 La gestione dei dati su PC è demandata all'utente utilizzatore che dovrà provvedere a memorizzare sulle condivisioni aziendali dati che possono essere utilizzati anche da altri utenti, evitando di mantenere l'esclusività su di essi. Non è consentita l'installazione di programmi diversi da quelli autorizzati dall'Ufficio Sistemi Informativi Informativi o dall'apposito incaricato.

6.9 Gli operatori dell'Ufficio Sistemi Informativi Informativi o l'apposito incaricato possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la sicurezza dei PC, della rete locale e dei server aziendali, nonché tutte le impostazioni eventualmente configurate che possano interferire con il corretto funzionamento dei servizi informatici aziendali.

6.10 È obbligatorio consentire l'installazione degli aggiornamenti di sistema che vengono proposti automaticamente, al primo momento disponibile, in modo tale da mantenere il PC sempre protetto.

6.11 È vietato utilizzare il PC per l'acquisizione, la duplicazione e/o la trasmissione illegale di opere protette da copyright.

6.12 È vietato l'utilizzo di supporti di memoria (chiavi USB, CD, DVD o altri supporti) per il salvataggio di dati trattati tramite gli Strumenti Aziendali, salvo che il supporto utilizzato sia

stato fornito dall'Ufficio Sistemi Informativi Informativi o dall'apposito incaricato. In tale caso, il supporto fornito può essere utilizzato esclusivamente per finalità lavorative.

6.13 È assolutamente vietato connettere al PC qualsiasi periferica non autorizzata preventivamente dall'Amministratore di Sistema.

6.14 È assolutamente vietato connettere alla rete locale qualsiasi dispositivo (PC esterni, router, switch, modem, etc.) non autorizzato preventivamente dall'Amministratore dei Sistemia Informativi o dall'apposito incaricato.

6.15 Nel caso in cui l'utente dovesse notare comportamenti anomali del PC, l'utente stesso è tenuto a comunicarlo tempestivamente all'Ufficio Sistemi Informativi Informativi o all'apposito incaricato.

I log relativi all'utilizzo di Strumenti, reperibili nella memoria degli Strumenti stessi ovvero sui Server o sui router aziendali, nonché i file con essi trattati sono registrati e possono essere oggetto di controllo da parte del Titolare del trattamento, attraverso l'Ufficio Sistemi Informativi aziendale Informativi o l'apposito incaricato, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale.
I controlli possono avvenire secondo le disposizioni previste al successivo punto 12 del presente Regolamento.
Le informazioni così raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 679/16 "General Data Protection".

7 - Utilizzo di internet

Le regole di seguito specificate sono adottate anche ai sensi delle "Linee guida del Garante per posta elettronica e internet" pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007.
Ciascun dipendente /collaboratore si deve attenere alle seguenti regole di utilizzo della rete Internet e dei relativi servizi.

7.1 È ammessa solo la navigazione in siti considerati correlati con la prestazione lavorativa. L'accesso è consentito dal firewall aziendale con le sue policy di sicurezza debitamente implementate e aggiornate, ad es. i siti istituzionali, i siti degli Enti locali, di fornitori e partner aziendali.

7.2 È vietato compiere azioni che siano potenzialmente in grado di arrecare danno all'Ente, ad esempio, il download o l'upload di file audio e/o video, l'uso di servizi di rete con finalità ludiche o, comunque, estranee all'attività lavorativa.

7.3 È vietato a chiunque il download di qualunque tipo di software gratuito (freeware) o shareware prelevato da siti Internet, se non espressamente autorizzato dagli Amministratori di Sistema Informativi o dall'apposito incaricato.

7.4 L'Ente si riserva di bloccare l'accesso a siti "a rischio" attraverso l'utilizzo di blacklist pubbliche in continuo aggiornamento e di predisporre filtri, basati su sistemi euristici di valutazione del livello di sicurezza dei siti web remoti, tali da prevenire operazioni potenzialmente pericolose o comportamenti impropri. In caso di blocco accidentale di siti di interesse aziendale l'interessato dovrà contattare l'Ufficio Sistemi Informativi Informativi o l'apposito incaricato per uno sblocco selettivo.

7.5 Nel caso in cui, per ragioni di servizio, si necessiti di una navigazione libera dai filtri del suddetto firewall, è necessario richiedere lo sblocco mediante una mail al responsabile dell'ufficio/servizio, nella quale siano indicati chiaramente: motivo della richiesta, utente e postazione da cui effettuare la navigazione libera, intervallo di tempo richiesto per completare l'attività. L'utente, nello svolgimento delle proprie attività, deve comunque tenere presente in

modo particolare i punti 10 del presente regolamento. Al termine dell'attività gli addetti dell'Ufficio Sistemi Informativi ripristineranno i filtri nella situazione iniziale.

7.6 È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo i casi direttamente autorizzati dal responsabile dell'ufficio/servizio, con il rispetto delle normali procedure di acquisto.

7.7 È assolutamente vietata la partecipazione a Forum non professionali, ai Social Network, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

7.8 È consentito l'uso di strumenti di messaggistica istantanea, per permettere una efficace e comoda comunicazione tra i colleghi, mediante i soli strumenti autorizzati dall'Ufficio Sistemi Informativi o dall'apposito incaricato. Tali strumenti hanno lo scopo di migliorare la collaborazione tra utenti aggiungendo un ulteriore canale comunicativo rispetto agli spostamenti fisici, alle chiamate telefoniche ed e-mail. È consentito un utilizzo legato esclusivamente a scopi professionali. Anche su tali strumenti di messaggistica istantanea è attivo il monitoraggio e la registrazione dell'attività degli utenti, secondo le disposizioni dei punti 10 del presente regolamento.

7.9 Per motivi tecnici e di buon funzionamento del sistema informatico è buona norma, salvo comprovata necessità, non accedere a risorse web che impegnino in modo rilevante banda, come a titolo esemplificativo: filmati (tratti da youtube, siti di informazione, siti di streaming ecc) o web radio, in quanto possono limitare e/o compromettere l'uso della rete agli altri utenti.

8 - Utilizzo della posta elettronica

Le regole di seguito specificate sono adottate anche ai sensi delle "Linee guida del Garante per posta elettronica e internet" pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007.
Ciascun dipendente/collaboratore si deve attenere alle seguenti regole di utilizzo dell'indirizzo di Posta elettronica.

8.1 Ad ogni utente viene fornito un account e-mail aziendale nominativo, generalmente coerente con il modello *nome.cognome@aato.venetoriental.it.* L'utilizzo dell'e-mail deve essere limitato esclusivamente a scopi aziendali, ed è assolutamente vietato ogni utilizzo di tipo privato. L'utente a cui è assegnata una casella di posta elettronica è responsabile del corretto utilizzo della stessa.

8.2 L'Ente fornisce, altresì, delle caselle di posta elettronica associate a ciascuna unità organizzativa, ufficio o gruppo di lavoro il cui utilizzo è da preferire rispetto alle e-mail nominative qualora le comunicazioni siano di interesse collettivo: questo per evitare che degli utenti singoli mantengano l'esclusività su dati aziendali.

8.3 L'iscrizione a mailing-list o newsletter esterne con il proprio indirizzo aziendale personale è concessa esclusivamente per motivi professionali. Prima di iscriversi occorre verificare anticipatamente l'affidabilità del sito che offre il servizio.

8.4 Allo scopo di garantire sicurezza alla rete aziendale, evitare di aprire messaggi di posta in arrivo da mittenti di cui non si conosce l'identità o con contenuto sospetto o insolito, oppure che contengano allegati di tipo *.exe, *.com, *.vbs, *.htm, *.scr, *.bat, *.js e *.pif. È necessario porre molta attenzione, inoltre, alla credibilità del messaggio e del mittente per evitare casi di phishing o frodi informatiche. In qualunque situazione di incertezza contattare gli Amministratori di Sistema o l'Ufficio Sistemi Informativi o l'apposito incaricato per una valutazione dei singoli casi.

8.5 Non é consentito diffondere messaggi del tipo "catena di S. Antonio" o di tipologia simile anche se il contenuto sembra meritevole di attenzione; in particolare gli appelli di solidarietà e i messaggi che informano dell'esistenza di nuovi virus. In generale è vietato l'invio di messaggi pubblicitari di prodotti di qualsiasi tipo.

8.6 Nel caso fosse necessario inviare allegati "pesanti" (fino al 25 MB) è opportuno ricorrere prima alla compressione dei file originali in un archivio di formato .zip o equivalenti (da chiarire). Nel caso di allegati ancora più voluminosi è necessario rivolgersi all'Ufficio Sistemi Informativi o all'apposito incaricato.

8.7 Nel caso in cui fosse necessario inviare a destinatari esterni messaggi contenenti allegati con dati personali o dati personali sensibili, è obbligatorio che questi allegati vengano preventivamente resi inintelligibili attraverso crittazione con apposito software (archiviazione e compressione con password). La password di crittazione deve essere comunicata al destinatario attraverso un canale diverso dalla mail (ad esempio per lettera o per telefono) e mai assieme ai dati criptati. Tutte le informazioni aziendali, i dati personali e/o sensibili di competenza aziendale possono essere inviati soltanto a destinatari - persone o Enti – qualificati e competenti.(da chiarire)

8.8 Non è consentito l'invio automatico di e-mail all'indirizzo e-mail privato (attivando per esempio un "inoltro" automatico delle e-mail entranti), anche durante i periodi di assenza (es. ferie, malattia, infortunio ecc.). In questa ultima ipotesi, è raccomandabile utilizzare un messaggio "Out of Office" facendo menzione di chi, all'interno dell'Ente, assumerà le mansioni durante l'assenza, oppure indicando un indirizzo di mail alternativo preferibilmente di tipo collettivo, tipo ufficioXXX@aato.venetoriental.it. Rivolgersi all'Ufficio Sistemi Informativi o all'apposito incaricato per tale eventualità.

8.9 In caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, qualora non fosse possibile attivare la funzione autoreply o l'inoltro automatico su altre caselle aziendali e si debba conoscere il contenuto dei messaggi di posta elettronica, il titolare della casella di posta ha la facoltà di delegare un altro dipendente (fiduciario) per verificare il contenuto di messaggi e per inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Sarà compito del responsabile assicurarsi che sia redatto un verbale attestante quanto avvenuto e che sia informato il lavoratore interessato alla prima occasione utile;

8.10 La diffusione massiva di messaggi di posta elettronica deve essere effettuata esclusivamente per motivi inerenti il servizio, possibilmente su autorizzazione del responsabile competente. Per evitare che le eventuali risposte siano inoltrate a tutti, generando traffico eccessivo ed indesiderato, i destinatari dovranno essere messi in copia nascosta (Bcc o Ccn) se la tipologia del messaggio lo consente.

8.11 È vietato inviare posta elettronica in nome e per conto di un altro utente, salvo sua espressa autorizzazione;

8.12 La casella di posta elettronica personale deve essere mantenuta in ordine, cancellando messaggi e documenti la cui conservazione non è più necessaria. Anche la conservazione di messaggi con allegati pesanti è da evitare per quanto possibile, preferendo, in alternativa, il salvataggio dell'allegato sulle condivisioni aziendali.

8.13 I messaggi in entrata vengono sistematicamente analizzati alla ricerca di virus e malware e per l'eliminazione dello spam. I messaggi che dovessero contenere virus vengono eliminati dal sistema e il mittente/destinatario viene avvisato mediante messaggio specifico.

Si informa che l'Ente, per il tramite dell'Ufficio Sistemi Informativi o dell'apposito incaricato, non controlla sistematicamente il flusso di comunicazioni mail né è dotato di sistemi per la lettura o analisi sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail.

Tuttavia, in caso di assenza improvvisa o prolungata del dipendente ovvero per imprescindibili esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale ovvero per motivi di sicurezza del sistema informatico, l'Ente per il tramite dell'Ufficio Sistemi Informativi può, secondo le procedure indicate successivo punto 12 del presente Regolamento, accedere all'account di posta elettronica aziendale, prendendo visione dei messaggi, salvando o cancellando file.
Si informa che, in caso di cessazione del rapporto lavorativo, la mail aziendale affidata all'incaricato verrà sospesa per un periodo di **3 mesi** e successivamente disattivata. Nel periodo di sospensione l'account rimarrà attivo e visibile ad un soggetto incaricato dall'Ente solo in ricezione, che tratterà i dati e le informazioni pervenute per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale, trasmettendone il contenuto ad altri dipendenti (se il messaggio ha contenuto lavorativo) ovvero cancellandolo (se il messaggio non ha contenuto lavorativo). Il sistema in ogni caso genererà una risposta automatica al mittente, invitandolo a reinviare il messaggio ad altro indirizzo mail aziendale.
Le informazioni eventualmente raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 679/16 "General Data Protection".

9 Utilizzo dei telefoni, fax, fotocopiatrici, scanner e stampanti aziendali

Il dipendente è consapevole che gli Strumenti di stampa, così come anche il telefono dell'Ente, sono di proprietà del CONSIGLIO DI BACINO VENETO ORIENTALE e sono resi disponibili all'utente per rendere la prestazione lavorativa. Pertanto ne viene concesso l'uso esclusivamente per tale fine.

9.1 Il telefono aziendale affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa e non sono quindi consentite comunicazioni a carattere personale e/o non strettamente inerenti l'attività lavorativa stessa. La ricezione o l'effettuazione di comunicazioni a carattere personale è consentito solo nel caso di comprovata necessità ed urgenza.

9.2 Qualora venisse assegnato un cellulare aziendale all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Ai cellulari e smartphone aziendali si applicano le medesime regole sopra previste per gli altri dispositivi informatici (cfr. 6 "Utilizzo di personal computer"), per quanto riguarda il mantenimento di un adeguato livello di sicurezza informatica. In particolare si raccomanda il rispetto delle regole per una corretta navigazione in Internet (cfr. 8), se consentita.

9.3 Per gli smartphone aziendali è vietata l'installazione e l'utilizzo di applicazioni (o altresì denominate "app" nel contesto degli smartphone) diverse da quelle autorizzate dall'Ufficio Sistemi informativi.

9.4 È vietato l'utilizzo dei fax aziendali per fini personali, tanto per spedire quanto per ricevere documentazione, fatta salva esplicita autorizzazione da parte del Responsabile di Ufficio.

9.5 È vietato l'utilizzo delle fotocopiatrici aziendali per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile di Ufficio.

9.6 Per quanto concerne l'uso delle stampanti gli utenti sono tenuti a:

9.6.1 Stampare documenti solo se strettamente necessari per lo svolgimento delle proprie funzioni operative

9.6.2 Prediligere le stampanti di rete condivise, rispetto a quelle locali/personali, per ridurre l'utilizzo di materiali di consumo (toner ed altri consumabili)

9.6.3 Prediligere la stampa in bianco/nero e fronte/retro al fine di ridurre i costi, se possibile.

9.7 Le stampanti e le fotocopiatrici aziendali devono essere spente ogni sera prima di lasciare gli uffici o in caso di inutilizzo prolungato.

9.8 Nel caso in cui si rendesse necessaria la stampa di informazioni riservate l'utente dovrà presidiare il dispositivo di stampa per evitare la possibile perdita o divulgazione di tali informazioni e persone terze non autorizzate.

10 - Assistenza agli utenti e manutenzioni

10.1 L'Ufficio Sistemi informativi e gli Amministratori di Sistema o l'apposito incaricato possono accedere ai dispositivi informatici aziendali sia direttamente, sia mediante software di accesso remoto, per i seguenti scopi:

10.1.1 – verifica e risoluzione di problemi sistemistici ed applicativi, su segnalazione dell'utente finale.

10.1.2 – verifica del corretto funzionamento dei singoli dispositivi in caso di problemi rilevati nella rete.

10.1.3 – richieste di aggiornamento software e manutenzione preventiva hardware e software.

10.2 Gli interventi tecnici posso avvenire previo consenso dell'utente, quando l'intervento stesso richiede l'accesso ad aree personali dell'utente stesso. Qualora l'intervento tecnico, in loco o in remoto, non necessiti di accedere mediante credenziali utente, gli Amministratori di sistema o l'apposito incaricato sono autorizzati ad effettuare gli interventi senza il consenso dell'utente cui la risorsa è assegnata.

10.3 L'accesso in teleassistenza sui PC della rete aziendale richiesto da terzi (fornitori e/o altri) deve essere autorizzato dall'Amministratore di Sistema o dall'apposito incaricato, per le verifiche delle modalità di intervento per il primo accesso. Le richieste successive, se effettuate con la medesima modalità, possono essere gestite autonomamente dall'utente finale.

10.4 Durante gli interventi in teleassistenza da parte di operatori terzi, l'utente richiedente o gli Amministratori di Sistema o l'apposito incaricato devono presenziare la sessione remota, in modo tale da verificare ed impedire eventuali comportamenti non conformi al presente regolamento.

11 Controlli sugli Strumenti (art. 6.1 Provv. Garante, ad integrazione dell'Informativa ex art. 13 Reg. 679/16)

11.1 Poiché in caso di violazioni contrattuali e giuridiche, sia l'Ente, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, l'Ente verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico. Il datore di lavoro, infatti, può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori (art. 4, comma2), di sistemi che consentono indirettamente il controllo a distanza (c.d. controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori. Resta ferma la necessità di rispettare le procedure di informazione e di consultazione di lavoratori e sindacati in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati, nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori. I controlli devono essere effettuati nel rispetto dell'art. 1.2 del presente Regolamento e dei seguenti principi:

- **Proporzionalità:** il controllo e l'estensione dello stesso dovrà rivestire, in ogni caso, un carattere adeguato, pertinente e non eccessivo rispetto alla/alle finalità perseguite, ma resterà sempre entro i limiti minimi.
- **Trasparenza:** l'adozione del presente Regolamento ha l'obiettivo di informare gli utenti sui diritti ed i doveri di entrambe le parti.
- **Pertinenza e non eccedenza:** ovvero evitando un'interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, così come la possibilità di controlli prolungati, costanti o indiscriminati.

11.2 L'uso degli Strumenti Informatici dell'Ente può lasciare traccia delle informazioni sul relativo uso, come analiticamente spiegato nei riquadri di cui ai punti 6 – 7 – 8 – 9 del presente Regolamento. Tali informazioni, che possono contenere dati personali eventualmente anche sensibili dell'Utente, possono essere oggetto di controlli da parte dell'Ente, per il tramite dell'Amministratore di Sistema o dell'apposito incaricato, volti a garantire esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale, nonché per la sicurezza e la salvaguardia del sistema informatico, per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento / sostituzione / implementazione di programmi, manutenzione hardware, etc.). Gli interventi di controllo sono di due tipi (di seguito descritti al punto 12) e possono permettere all'Ente di prendere indirettamente cognizione dell'attività svolta con gli strumenti.

11.3 ***Controlli per la tutela del patrimonio aziendale, nonché per la sicurezza e la salvaguardia del sistema informatico. Controlli per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, ecc.).***

Qualora per le finalità qui sopra descritte risulti necessario l'accesso agli Strumenti e alle risorse informatiche e relative informazioni descritte ai punti 6 – 7 – 8 – 9 il Responsabile del trattamento dei dati personali per il tramite dell'Ufficio Sistemi informativi o dell'apposito incaricato, si atterrà al processo descritto qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo).

i. Avviso generico a tutti i dipendenti della presenza di comportamenti anomali che possono mettere a rischio la sicurezza del sistema informativo e richiamo all'esigenza di attenersi al rispetto del presente Regolamento.
ii. Successivamente, dopo almeno 7 giorni, se il comportamento anomalo persiste, l'Ente potrà autorizzare il personale addetto al controllo, potendo così accedere alle informazioni descritte ai punti 6 – 7 – 8 – 9 con possibilità di rilevare files trattati, siti web visitati, software installati, documenti scaricati, statistiche sull'uso di risorse ecc. nel corso dell'attività lavorativa. Tale attività potrà essere effettuata in forma anonima ovvero tramite controllo del numero IP, dell'Utente e con l'identificazione del soggetto che non si attiene alle istruzioni impartite.
iii. Qualora il rischio di compromissione del sistema informativo aziendale sia imminente e grave a tal punto da non permettere l'attesa dei tempi necessari per i passaggi procedimentali descritti ai punti 1 e 2, il Responsabile del Trattamento, unitamente all'amministratore di sistema o all'apposito incaricato, può intervenire senza indugio sullo strumento da cui proviene la potenziale minaccia.

12 Controlli per esigenze produttive e di organizzazione

Per esigenze produttive e di organizzazione si intendono – fra le altre – l'urgente ed improrogabile necessità di accedere a files o informazioni lavorative di cui si è ragionevolmente certi che siano

disponibili su risorse informatiche di un Utente (quali file salvati, posta elettronica, chat, SMS, ecc) che non sia reperibile, in quanto ad esempio assente, temporaneamente irreperibile ovvero cessato.
Qualora risulti necessario l'accesso alle risorse informatiche e relative informazioni descritte ai punti 6 – 7 – 8 – 9 il Responsabile del trattamento dei dati personali, per il tramite dell'Ufficio Sistemi informativi o dell'apposito incaricato, si atterrà alla procedura descritta qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo).

i. Redazione di un atto da parte del responsabile dell'ufficio/servizio che comprovi le necessità produttive e di organizzazione che richiedano l'accesso allo Strumento.
ii. Incarico all'Amministratore di sistema o all'apposito incaricato di accedere alla risorsa con credenziali di Amministratore ovvero tramite l'azzeramento e la contestuale creazione di nuove credenziali di autenticazione dell'Utente interessato, con avviso che al primo accesso alla risorsa, lo stesso dovrà inserire nuove credenziali.
iii. Redazione di un verbale che riassuma i passaggi precedenti.
iv. In ogni caso l'accesso ai documenti presenti nella risorsa è limitato a quanto strettamente indispensabile alle finalità produttive e di organizzazione del lavoro.
v. Qualora indirettamente si riscontrino file o informazioni anche personali, esse potranno essere altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, considerato che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Regolamento Europeo 679/16 "General Data Protection".

Tutti i controlli sopra descritti avvengono nel rispetto del principio di necessità e non eccedenza rispetto alle finalità descritte nel presente Regolamento. Dell'attività sopra descritta viene redatto verbale, sottoscritto dal Responsabile del Trattamento e dall'Amministratore di Sistema o dall'apposito incaricato che ha svolto l'attività.
In caso di nuovo accesso da parte dell'utente allo Strumento informatico oggetto di controllo, lo stesso dovrà avvenire previo rilascio di nuove credenziali (salvo diverse esigenze tecniche).
Qualora indirettamente si riscontrino file o informazioni anche personali, esse potranno essere altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, considerato che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Regolamento Europeo 679/16 "General Data Protection".

13 - Conservazione dei dati

13.1 In riferimento agli articoli 5 e 6 del Reg. 679/16 e in applicazione ai principi di diritto di accesso, legittimità, proporzionalità, sicurezza ed accuratezza e conservazione dei dati, le informazioni relative all'accesso ad Internet e dal traffico telematico (log di sistema e del firewall), la cui conservazione non sia necessaria, saranno cancellati entro dodici mesi dalla loro produzione

13.2 In casi eccezionali – ad esempio: per esigenze tecniche o di sicurezza; o per l'indispensabilità dei dati rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria o, infine, all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria – è consentito il prolungamento dei tempi di conservazione limitatamente al soddisfacimento delle esigenze sopra esplicitate.

13.3 La Ente si impegna ad assumere le misure di sicurezza nel trattamento e nella conservazione di tale tipologia di dati alla luce di quanto stabilito dal Legislatore.

14 - Partecipazioni a Social Media

14.1 L'utilizzo di Facebook, Twitter, Linkedin, dei blog e dei forum, anche professionali (ed altri siti o social media), al fine di promuovere attività istituzionali, è disciplinato da specifiche direttive ed istruzioni operative fornite al personale espressamente incaricato, rimanendo escluse iniziative individuali da parte dei singoli utenti o collaboratori.

14.2 Fermo restando il diritto della persona alla libertà di espressione, l'Ente ritiene comunque opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare tanto la propria immagine ed il patrimonio aziendale, anche immateriale, quanto i propri collaboratori, oltre che gli stessi utenti utilizzatori dei social media, fermo restando che è vietata la partecipazione agli stessi social media durante l'orario di lavoro.

14.3 Il presente articolo deve essere osservato dall'Utente sia che utilizzi dispositivi messi a disposizione dall'Ente, sia che utilizzi propri dispositivi, sia che partecipi ai social media a titolo personale, sia che lo faccia per finalità professionali, come dipendente dell'Ente.

14.4 La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni aziendali considerate dall'Ente riservate ed in genere, a titolo esemplificativo e non esaustivo, sulle informazioni inerenti attività, dati contabili, finanziari, progetti, procedimenti svolti o in svolgimento presso gli uffici. Inoltre, ogni comunicazione e divulgazione di contenuti dovrà essere effettuata nel pieno rispetto dei diritti di proprietà industriale e dei diritti d'autore, sia di terzi che dell'Ente. L'utente, nelle proprie comunicazioni, non potrà quindi inserire il nominativo e il logo dell'Ente, né potrà pubblicare disegni, modelli od altro connesso ai citati diritti. Ogni deroga a quanto sopra disposto potrà peraltro avvenire solo previa specifica autorizzazione dell'Amministrazione.

14.5 L'utente deve garantire la tutela della riservatezza e dignità delle persone; di conseguenza, non potrà comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci) di colleghi e in genere di collaboratori aziendali, se non con il preventivo personale consenso di questi, e comunque non potrà postare nei social media immagini, video, suoni e voci registrati all'interno dei luoghi di lavoro aziendali, se non con il preventivo consenso del Responsabile d'ufficio.

14.6 Qualora l'utente intenda usare social network, blog, forum su questioni anche indirettamente professionali (es. post su prodotti, servizi, fornitori, partner, ecc.) egli esprimerà unicamente le proprie opinioni personali; pertanto, ove necessario od opportuno per la possibile connessione con l'Ente, in particolare in forum professionali, l'utente dovrà precisare che le opinioni espresse sono esclusivamente personali e non riconducibili all'Ente.

15 - Sanzioni disciplinari

15.1 È fatto obbligo a tutti i dipendenti/collaboratori/utenti di osservare le disposizioni portate a conoscenza con il presente Regolamento. Eventuali violazioni del presente Regolamento da parte dei dipendenti nonché di altre norme previste dal CCNL applicato, a seconda della gravità della infrazione, comportano l'adozione dei seguenti provvedimenti:

- censura scritta;
- sospensione dal servizio;
- licenziamento in tronco;
- licenziamento di diritto.

Rimane comunque riservato il diritto di intraprendere azioni civili e penali nei confronti dei responsabili di qualsivoglia violazione a danno dell'Ente.

16 - Disposizioni finali

a) La pubblicizzazione del presente regolamento, a cura dell'Ufficio Sistemi Informativi, avverrà nelle seguenti forme: trasmissione per posta elettronica interna ai Responsabili, e a tutti gli impiegati provvisti di e-mail aziendale; attraverso la rete informatica interna, mediante affissione nei luoghi di lavoro con modalità analoghe a quelle previste dall'art. 7 dello Statuto dei lavoratori.

b) Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni e modifiche al presente Regolamento tramite comunicazione al responsabile dell'ufficio/servizio

Legenda

Amministratore di Sistema - E' il gestore del Sistema Informatico. I principali compiti dell'amministratore di sistema sono: installare e configurare nuovo hardware/software sia lato client (host) che lato server, rispondere alle esigenze della direzione della struttura gestita (azienda, ente statale, università, ecc.) (es. vincoli prestazionali e di affidabilità, rispetto di policy di sicurezza ecc...), ottenere le migliori prestazioni possibili con l'hardware a disposizione (ottimizzazione delle risorse), eseguire configurazioni di sistema opportune o desiderate in rispettivi file di configurazione, gestire gli account utente, pianificare e verificare la corretta esecuzione di operazioni pianificate come ad es. backup, applicare le patch e gli aggiornamenti necessari ai sottosistemi, rendere costantemente disponibili i servizi associati al sistema a favore degli utenti, analizzare i cosiddetti file di log, porre rimedio ai problemi/guasti tramite tecniche di troubleshooting, monitorare la struttura e gli apparati di rete in collaborazione con l'amministratore di rete, rispondere ai quesiti degli utenti, documentare le operazioni effettuate.

BIOS – Software di basso livello che fornisce ad un PC le funzioni di base per l'accesso all'hardware. E' il primo programma eseguito all'accensione, ancor prima del sistema operativo.

Chat line - Il termine chat (in inglese, letteralmente, "chiacchierata"), viene usato per riferirsi a un'ampia gamma di servizi sia telefonici che via Internet; ovvero, complessivamente, quelli che i paesi di lingua inglese distinguono di solito con l'espressione "online chat", "chat in linea". Questi servizi, anche piuttosto diversi fra loro, hanno tutti in comune due elementi fondamentali: il fatto che il dialogo avvenga in tempo reale, e il fatto che il servizio possa mettere facilmente in contatto perfetti sconosciuti, generalmente in forma essenzialmente anonima. Il "luogo" (lo spazio virtuale) in cui la chat si svolge è chiamato solitamente chatroom (letteralmente "stanza delle chiacchierate"), detto anche channel (in italiano canale), spesso abbreviato chan.

Download o upload - In generale con questo termine si intende il trasferimento di dati da un computer locale a uno remoto utilizzando un apparato di comunicazione, ad es. il modem, o tra computer della stessa rete. Per download si intende anche la visualizzazione sul proprio computer del contenuto di una pagina internet.

Firewall - E' un componente per la sicurezza informatica con lo scopo di controllare gli accessi alle risorse di un sistema filtrando tutto il traffico che tale sistema scambia con l'esterno. Il sistema, che si suppone sicuro e attendibile, protetto dal firewall può essere un singolo computer o una rete di computer (detta rete interna o rete locale o rete privata) mentre l'ambiente esterno con cui interagisce è tipicamente una rete che si suppone sconosciuta, insicura e non attendibile (detta rete esterna o rete pubblica. Un firewall filtra il traffico sulla base di un insieme di regole che definiscono una policy di sicurezza.

Forum – struttura informatica che consente la discussione online, tramite internet, degli utenti. Utilizzato per la discussione su temi specifici.

Guest book - Fornisce ai visitatori l'opportunità di lasciare commenti (sul sito) per i nuovi utenti che entreranno nel sito

Mailing list – Sistema organizzato per la partecipazione di più persone in una discussione asincrona mediante e-mail.

Malware – Software creato con l'intento di causare danni ad un sistema informatico o di carpire dati personali memorizzati in un sistema informatico.

Newsletter – notiziario scritto diffuso tramite e-mail agli utenti iscritti.

Phishing – attività illegale che sfrutta messaggi di posta elettronica ingannevoli per ottenere l'accesso a informazioni personale anche di carattere riservato, con la finalità del furto di identità nell'ambito di comunicazioni elettroniche. Utenti truffatori inviano messaggi che imitano logo e grafica di siti istituzionali con richieste di inserimento di dati personali, come numeri di carta di credito, codici personali e segreti di accesso etc. Si possono individuare da un attento esame del contenuto del messaggio che spesso contiene collegamenti a siti non istituzionali.

Remote banking - Per remote banking si intende l'insieme di servizi automatizzati che permettono ai clienti, grazie all'uso di terminali o di un semplice telefono, di collegarsi alla banca presso la quale intrattengono il conto corrente ed effettuare una serie di operazioni bancarie oppure di ricevere informazioni in tempo reale. A seconda del mezzo di comunicazione utilizzato si può parlare di phone banking ed internet banking.
Social network – servizio online che consiste nella connessione di persone legate da diversi legami sociali, quali interessi comuni, rapporti di lavoro, legami affettivi fino alla conoscenza casuale.
spam – messaggi di posta elettronica non sollecitati con contenuto generalmente commerciale.
***.exe, *.com, *.vbs, *.htm, *.scr, *.bat, *.js e *.pif** - Si tratta di estensioni di file che mandano in esecuzione file eseguibili che, a loro volta, possono infettare il computer con un virus.

Allegati

Estratto dalla Legge 20 maggio 1970, n. 300 (Statuto dei lavoratori) Norme sulla tutela della libertà e dignità del lavoratore, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento (così come modificato dall'art. 23, D.Lgs. n. 151/2015)

ART. 4 - Impianti audiovisivi e altri strumenti di controllo

Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo gli impianti e gli strumenti di cui al periodo precedente possono essere installati previa autorizzazione della Direzione territoriale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più Direzioni territoriali del lavoro, del Ministero del lavoro e delle politiche sociali. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal Regolamento Europeo 679/16 "General Data Protection".

ART. 7. - Sanzioni disciplinari.

Le norme disciplinari relative alle sanzioni, alle infrazioni in relazione alle quali ciascuna di esse può essere applicata ed alle procedure di contestazione delle stesse, devono essere portate a conoscenza dei lavoratori mediante affissione in luogo accessibile a tutti. Esse devono applicare quanto in materia è stabilito da accordi e contratti di lavoro ove esistano. Il datore di lavoro non può adottare alcun provvedimento disciplinare nei confronti del lavoratore senza avergli preventivamente contestato l'addebito e senza averlo sentito a sua difesa. Il lavoratore potrà farsi assistere da un rappresentante dell'associazione sindacale cui aderisce o conferisce mandato. Fermo restando quanto disposto dalla legge 15 luglio 1966, n. 604, non possono essere disposte sanzioni disciplinari che comportino mutamenti definitivi del rapporto di lavoro; inoltre la multa non può essere disposta per un importo superiore a quattro ore della retribuzione base e la sospensione dal servizio e dalla retribuzione per più di dieci giorni. In ogni caso, i provvedimenti disciplinari più gravi del rimprovero verbale non possono essere applicati prima che siano trascorsi cinque giorni dalla contestazione per iscritto del fatto che vi ha dato causa. Salvo analoghe procedure previste dai contratti collettivi di lavoro e ferma restando la facoltà di adire l'autorità giudiziaria, il lavoratore al quale sia stata applicata una sanzione disciplinare può promuovere, nei venti giorni successivi, anche per mezzo dell'associazione alla quale sia iscritto ovvero conferisca mandato, la costituzione, tramite l'ufficio provinciale del lavoro e della massima occupazione, di un collegio di conciliazione ed arbitrato, composto da un rappresentante di ciascuna delle parti e da un terzo membro scelto di comune accordo o, in difetto di accordo, nominato dal direttore dell'ufficio del lavoro. La sanzione disciplinare resta sospesa fino alla pronuncia da parte del collegio.

Qualora il datore di lavoro non provveda, entro dieci giorni dall'invito rivoltogli dall'ufficio del lavoro, a nominare il proprio rappresentante in seno al collegio di cui al comma precedente, la sanzione disciplinare non ha effetto. Se il datore di lavoro adisce l'autorità giudiziaria, la sanzione

disciplinare resta sospesa fino alla definizione del giudizio. Non può tenersi conto ad alcun effetto delle sanzioni disciplinari decorsi due anni dalla loro applicazione.

PROPOSTA DI DELIBERAZIONE COMITATO ISTITUZIONALE PROT. N.415 DEL 22.05.2018

OGGETTO: **Regolamento per l'utilizzo dei sistemi informatici. Approvazione.**

PARERE DI REGOLARITA' TECNICO- CONTABILE

Il sottoscritto Bruno Palmieri Vice Direttore;

Vista la proposta di deliberazione di cui all'oggetto;

Visto l'art. 49, comma 1, del Decreto Legislativo 18 Agosto 2000 n. 267, "Testo unico delle leggi sull'ordinamento degli Enti Locali";

Esprime parere:

[X] **FAVOREVOLE**

Conegliano, 22.05.2018

IL VICE DIRETTORE
F.to Bruno Palmieri

Il presente processo verbale, viene chiuso e firmato a termini di legge dal Presidente e dal Direttore.

IL PRESIDENTE
F.to Ing. Fabio Vettori

IL DIRETTORE
F.to Dott. Agostino Battaglia

REFERTO DI PUBBLICAZIONE (art. 124 D.Lgs. 18.08.2000 n. 267)

Attesta il sottoscritto che copia del presente verbale sarà pubblicata all'Albo del Consiglio di Bacino Veneto Orientale Ambito Territoriale Ottimale per il servizio idrico integrato il giorno 24 MAG. 2018 e vi rimarrà affissa per 15 (quindici) giorni consecutivi ai sensi dell'art. 124, 2° comma, del D.Lgs. 18.08.2000 n. 267.

Conegliano, 24 MAG. 2018

IL VICE DIRETTORE
F.to Bruno Palmieri

PER COPIA CONFORME ALL'ORIGINALE

Conegliano, 24 MAG. 2018

IL VICE DIRETTORE
(Bruno Palmieri)

CERTIFICATO DI PUBBLICAZIONE ED ESECUTIVITA' (Art. 134 D.Lgs., 3° comma, del D.Lgs. 18.8.2000 n. 267)

Si certifica che la su estesa deliberazione è stata pubblicata all'Albo del Consiglio di Bacino Veneto Orientale Ambito Territoriale Ottimale per il servizio idrico integrato per 15 (quindici) giorni consecutivi, divenendo esecutiva il 04 GIU. 2018.

Conegliano, 08 GIU. 2018

IL VICE DIRETTORE
(Bruno Palmieri)