COMUNE DI RHO

Appendice al Regolamento sull'Ordinamento degli Uffici e Servizi
del Comune di Rho

DISCIPLINARE
PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI, DELLA POSTA ELETTRONICA E DI INTERNET

Adottato con deliberazione di Giunta comunale n. 56 del 05/03/2019 – esecutiva il 19/03/2019

Indice

Art. 1 - Finalità

1. Il presente Disciplinare (di seguito anche "Regolamento"), che integra il Regolamento sull'ordinamento degli Uffici e Servizi del Comune di Rho per quanto riguarda l'utilizzo degli Strumenti Informatici, è finalizzato a:
   - adottare indirizzi trasparenti, capaci di comunicare con estrema chiarezza agli utenti del sistema informatico comunale le corrette modalità di utilizzo degli strumenti informatici loro assegnati per lo svolgimento delle mansioni attribuite;
   - definire con altrettanta chiarezza il diritto dell'Amministrazione a verificare l'uso corretto dei suddetti strumenti;
   - individuare le modalità con cui l'Amministrazione esercita tale diritto di verifica.
2. La presente disciplina è diretta anche ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza del sistema informatico e dei dati in esso contenuti oppure scambiati ed ancora esporre il Comune ai rischi di un coinvolgimento sia patrimoniale che penale, creando anche conseguenti problemi di immagine.

Art. 2 - Campo di applicazione

1. La rete del Comune di Rho è costituita dall'insieme delle risorse informatiche, cioè dalle risorse infrastrutturali, e dal patrimonio informativo digitale. Le risorse infrastrutturali sono i server, i personal computer, notebook, sistema di posta elettronica ed altri strumenti con relativi software e applicativi (in seguito per brevità detti anche **"Strumenti"**). Il patrimonio informativo è l'insieme delle banche dati in formato digitale ed in generale tutti i documenti prodotti tramite l'utilizzo dei suddetti Strumenti.
2. Il presente disciplinare si applica a tutti gli utenti che a diverso titolo sono autorizzati ad accedere alla rete comunale. Per utenti si intendono, quindi, tutti i dipendenti a tempo indeterminato e determinato, senza distinzione di ruolo e/o livello, nonché tutti i collaboratori dell'Ente, a prescindere dal rapporto contrattuale con gli stessi intrattenuto, e gli utenti esterni. Per utenti esterni si intendono tutti i soggetti che usufruiscono dei sistemi informativi per erogare un servizio pubblico (ad esempio utenti abilitati per consultazioni anagrafiche).
3. Sono esentati dall'applicazione del presente Regolamento, limitatamente a quanto necessario per il corretto svolgimento delle proprie funzioni, i dipendenti del Sistema

Informativo Comunale e/o incaricati esterni individuati quali Amministratori di Sistema.

4. Gli Amministratori (sindaco, assessori, …) ai quali siano messi a disposizione per l'espletamento dei compiti connessi alla loro funzione i servizi di accesso ad internet e/o di utilizzo della posta elettronica e/o di altri Strumenti, sono tenuti al rispetto delle regole contenute nel presente Regolamento.

Art. 3 – Proprietà intellettuale e licenze

1. Qualsiasi software in uso nel sistema informatico comunale per il quale sia prevista una licenza d'uso deve essere ottenuto seguendo le procedure di acquisizione definite dai regolamenti interni e deve essere registrato a nome del Comune di Rho.
2. Il software che non richieda una licenza d'uso a titolo oneroso, quale quello a sorgente aperta (open source) o il software distribuito con licenza d'uso di tipo freeware o shareware, deve essere selezionato o comunque sottoposto al vaglio del Sistema Informativo Comunale.
3. Non è possibile installare, duplicare o utilizzare software acquisiti al di fuori di quanto consentito dagli accordi di licenza.
4. Tutti gli utenti sono tenuti al rispetto delle leggi in materia di tutela della proprietà intellettuale (copyright) sia per quanto riguarda il software che per quanto riguarda file multimediali.

Art. 4 – Utilizzo dei dati

1. I documenti, i dati e le informazioni detenute su apparecchiature o altri supporti di proprietà del Comune sono da considerare a pieno titolo beni comunali e vengono utilizzati dal personale, anche fuori dagli uffici comunali, ai soli fini lavorativi.
2. Nel caso in cui esista la necessità di elaborare banche dati in locale, ad esempio su fogli di calcolo o database personali, è necessario adottare le misure di sicurezza idonee a garantire il rispetto della normativa in materia di tutela dei dati personali.
3. I dati, documenti o file di qualsiasi genere, creati o modificati attraverso le applicazioni di produttività individuale (es. word, excel, ecc.) devono obbligatoriamente essere salvati solo sulle condivisioni di rete previste dall'articolo 9. Si ricorda che i dati contenuti nel computer locale sono maggiormente soggetti a perdita in caso di guasto del sistema in quanto non sottoposti al backup centralizzato previsto per le unità di rete. Il salvataggio e la salvaguardia dei dati presenti sul disco locale della postazione di

lavoro sono ad esclusiva cura dell'utente.

4. Nessun dato del Comune di Rho o personale degli utenti e di coloro che vengono in contatto a qualsiasi titolo con l'Amministrazione comunale, detenuto per esigenze connesse al servizio, può essere trattato o memorizzato su dispositivi di qualsiasi tipologia (es. dischetti CD, DVD, supporti USB) di proprietà dell'utente (vedi art. 10 comma 9). In ogni caso, si possono effettuare copie di dati su supporti rimovibili solo se autorizzati dal Responsabile di Servizio.
5. Tutti i supporti rimovibili (CD, DVD, supporti USB, ecc.) contenenti dati istituzionali qualificati come dati personali dalla normativa in materia di privacy, sia comuni che sensibili, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato. In alcuni casi, infatti, è possibile recuperare i dati memorizzati anche dopo la loro cancellazione. Per questo motivo il supporto, al termine dell'utilizzo, deve essere formattato prima di essere riutilizzato, oppure distrutto. A tal fine ciascun utente dovrà contattare il personale del Sistema Informativo Comunale e seguire le istruzioni da questo impartite.
6. In ogni caso, i supporti magnetici contenenti dati sensibili devono essere dagli utenti adeguatamente custoditi in armadi chiusi. L'utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.
7. E' vietato, salvo autorizzazione espressa del Sindaco quale Titolare del trattamento, salvare/stampare/inoltrare e portare fuori dai luoghi di lavoro documentazione dell'Ente. A titolo esemplificativo e non esaustivo è vietato:
    - inviare informazioni sensibili ad indirizzi di posta personali;
    - salvare documenti elettronici del Comune (ad esempio pervenuti via posta elettronica o salvati sul Server o sullo Strumento in dotazione) su repository esterne (quali ad esempio Dropbox, GoogleDrive, OneDrive, ecc.);
    - trasferire documenti elettronici dai sistemi informatici e Strumenti del Comune a device esterni ad uso personale (hard disk, chiavette, CD, DVD e altri supporti);
    - inoltrare a terzi estranei all'Ente documentazione interna/informazioni ricevute per mezzo di strumenti informatici o via cartacea, salvo che non sia funzionale allo svolgimento di prestazioni professionali a favore dello stesso Comune di Rho;

- stampare messaggi di posta elettronica di lavoro per scopi personali;
- fotocopiare/scansionare documentazione di lavoro per scopi personali.

Art. 5 – Accesso ai dati trattati dall'utente

1. Il Comune di Rho informa che il personale tecnico del Sistema Informativo Comunale e/o delle aziende che assicurano la manutenzione dei software/hardware in uso nell'Ente può accedere ai dati trattati dall'utente attraverso gli Strumenti aziendali, anche collegandosi in remoto alle singole postazioni e visualizzando il desktop. Il personale incaricato accederà ai dati su richiesta dell'utente e/o previo avviso al medesimo, in casi di particolare urgenza, l'avviso sarà successivo all'intervento ove possibile.
2. L'accesso è consentito esclusivamente per motivi di sicurezza e protezione del sistema informatico (ad es. contrasto virus, malware, intrusioni telematiche, fenomeni quali spamming, phishing, spyware, ecc.), ovvero per motivi tecnici e/o manutentivi e/o di regolare svolgimento dell'attività lavorativa (ad esempio: aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware).
3. La stessa facoltà di accesso ai dati, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Ente, si applica anche in caso di assenza prolungata od impedimento dell'utente.
4. Si informa altresì che l'uso degli Strumenti Informatici del Comune può lasciare traccia delle informazioni inerenti all'uso stesso attraverso la creazione di file di log, che possono contenere dati personali eventualmente anche sensibili dell'utente. I log relativi all'utilizzo di Strumenti sono reperibili nella memoria degli strumenti stessi oppure sui Server. Il personale tecnico del Sistema Informativo Comunale e/o delle aziende esterne incaricate può accedere a tali file di log sempre ai fini e con le modalità di cui ai punti da 1 a 3 del presente articolo.
5. Lo stesso personale tecnico, nei casi suindicati, può procedere a tutte le operazioni di configurazione e gestione necessarie a garantire la corretta funzionalità del sistema informatico aziendale, compresa la rimozione di file o applicazioni che riterranno pericolose per la sicurezza, sia sui singoli personal computer sia sulle unità di rete. Potrà altresì rimuovere dai personal computer tutte le impostazioni eventualmente configurate che possano interferire con il corretto funzionamento dei servizi informatici comunali. Le predette operazioni di rimozione avverranno previo avviso agli utenti, salvo

casi di particolare urgenza.

6. Ogni materiale personale rilevato dai tecnici di cui al presente articolo, a seguito di interventi di sicurezza informatica ovvero di manutenzione/aggiornamento su server ed anche su altri Strumenti dell'Ente, viene rimosso previo avviso agli utenti, salvo casi di particolare urgenza. Resta ferma ogni ulteriore responsabilità civile, penale e disciplinare.
7. È sempre fatta salva l'ipotesi di accesso ai dati, che trovino giustificazione nella necessità di rispondere ad eventuali richieste di organi di polizia e/o segnalazione dell'autorità giudiziaria o in presenza di sospetti relativamente all'esistenza di condotte improprie nell'uso degli Strumenti (cd. controlli difensivi).
8. L'accesso ai dati trattati dall'utente è possibile anche in occasione dei controlli di cui all'articolo 20.

Art. 6 – Gestione degli incidenti e violazione dei dati personali (databreach)

1. Nei casi in cui - a seguito di furti, attacchi informatici, accessi abusivi, incidenti o eventi avversi, come, incendi o altre calamità - si dovesse verificare la perdita, la distruzione o la diffusione indebita di dati personali conservati, trasmessi o comunque trattati (cd. "*databreach*") gli utenti devono segnalare senza indugio l'accaduto al proprio dirigente e al dirigente del Sistema informativo Comunale, che provvederanno tempestivamente ad informare il Sindaco, nella sua veste di Titolare del Trattamento, e il Responsabile protezione dati personali (RDP).
2. Nei casi di smarrimento o furto di strumenti informatici, il dirigente della struttura a cui è assegnata la strumentazione smarrita o sottratta dovrà anche sporgere denuncia all'Autorità Giudiziaria, avvisando anche l'Help desk dell'assistenza informatica per l'eventuale blocco dell'uso delle risorse informatiche.

Art. 7 – Cessazione del rapporto di lavoro

1. Al momento della cessazione del rapporto di lavoro, ovvero di qualunque evento che comporti la modifica delle funzioni precedentemente espletate, l'utente deve mettere a disposizione dell'Ente tutte le Risorse assegnate, sia in termini di attrezzature informatiche che di informazioni di interesse per i Servizi.
2. La fase di cessazione del rapporto di lavoro prevede le seguenti modalità operative:
   - le credenziali fornite all'utente verranno disabilitate: è cura del responsabile del

Servizio interessato comunicare le cessazioni degli utenti al Responsabile del Sistema Informativo Comunale;

- la casella di posta elettronica individuale verrà disattivata e i messaggi di posta elettronica sono conservati sino a 60 giorni dopo la cessazione del rapporto di lavoro: prima della cessazione dal servizio il dipendente è tenuto ad inoltrare al Responsabile del Servizio i messaggi di Posta Elettronica della propria casella con suffisso nome.cognome@comune.rho.mi.it contenenti documentazione relativa al Comune di Rho e rilevante ai fini istituzionali, compresi gli allegati;
- le eventuali registrazioni su siti e sistemi esterni, effettuate per motivi di servizio, dovranno essere portate a conoscenza del diretto Responsabile in tempo utile per consentire una loro migrazione verso altri utenti, ovvero la loro disabilitazione; il Segretario Comunale e i Dirigenti effettueranno tale comunicazione al Responsabile del Sistema Informativo comunale.

3. Le informazioni e i documenti prodotti o entrati nella disponibilità dell'utente nell'esercizio dell'attività lavorativa a favore del Comune di Rho restano nella piena ed esclusiva disponibilità del Comune.
4. L'utente non può formare, ottenere copia e/o cancellare documenti ed informazioni di interesse del Comune presenti sulle postazioni di lavoro o sulle risorse di rete, né farne alcun uso dopo la cessazione del rapporto di lavoro a meno di esplicita autorizzazione scritta preventiva da parte del Sindaco quale Titolare del trattamento.
5. Le informazioni eventualmente lasciate sulle postazioni di lavoro o sulle risorse di rete che non siano di interesse per il Comune potranno essere cancellate senza alcuna responsabilità per l'Ente.

Art. 8 – Gestione, assegnazione e revoca delle credenziali di accesso

1. I sistemi di controllo degli accessi assolvono il compito di prevenire che persone non autorizzate possano accedere a un sistema informatico ed alle relative applicazioni. Lo scopo è di cautelare il Comune ed i suoi dipendenti da ogni tipo di manomissione, furto o distruzione di dati oltre che di limitare l'accesso a specifici dati da parte di personale non autorizzato.
2. Le credenziali di accesso vengono assegnate al nuovo utente dal personale del Sistema Informativo Comunale, previa formale richiesta del Responsabile dell'ufficio/area

nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente.

3. Le ditte esterne ospitate nei locali comunali, così come il personale esterno incaricato dall'Ente (es. consulenti, stagisti, personale a tempo determinato), possono - previa autorizzazione - usufruire del sistema informatico comunale. Le richieste di autorizzazione all'accesso devono essere trasmesse dal dirigente del servizio interessato al responsabile del Sistema Informativo Comunale.
4. Le credenziali per il personale esterno di norma sono a tempo e quindi al momento della richiesta di rilascio deve essere indicata la data di scadenza (fine rapporto).
5. Si distinguono le credenziali di accesso alla rete e quelle di accesso ai programmi autorizzati, ciascuno con una specifica password, in particolare:
   - password di rete, per l'avvio e l'utilizzo del sistema operativo e di tutte le risorse di rete compresa la posta elettronica, ivi compresa la intranet;
   - password per l'accesso a particolari programmi e applicativi.
6. Le credenziali di autenticazione dell'utente (alla rete o ai programmi) costituite dalla coppia <User-id, Password>, vengono rilasciate dal Sistema Informativo Comunale secondo gli standard in uso nell'Ente e sono riconducibili alla seguente forma:
   - user-id
   - password alfanumerica inizializzata dal Sistema Informativo Comunale ed obbligatoriamente cambiata al primo utilizzo da parte dell'utente.
7. Al primo accesso al sistema l'utente è obbligato a cambiare la password assegnata di default e a porre in essere una gestione sicura della stessa nel rispetto dei seguenti requisiti:
   - la password deve essere diversa dallo User-ID;
   - deve avere lunghezza e caratteristiche tali da non essere facilmente identificata e/o deve essere conforme alle indicazioni date dalla procedura di impostazione password;
   - deve essere modificata secondo la procedura di modifica proposta automaticamente;
   - è fatto divieto all'utente di utilizzare password banali, ovvie, facilmente memorizzabili o agevolmente riconducibili all'utente;
   - la password non deve essere costituita da predefinite sequenze alfanumeriche,

né contenere riferimenti scontati o facilmente deducibili (nome del mese corrente, sequenze con numeri progressivi, ecc.) o riferimenti a carattere personale (date, numeri di telefono, nomi di persona, ecc.).

8. La coppia <User-id, Password> identifica univocamente l'utente. È assolutamente proibito entrare nella rete e nei programmi con le credenziali di altro utente.
9. Non è consentito accedere al programma di accensione delle stazioni di lavoro (Bios) e impostare protezioni o password ulteriori rispetto a quelle previste dal Sistema Informativo Comunale che limitino l'accesso alle stazioni di lavoro stesse.
10. L'utente è informato del fatto che la conoscenza di entrambe le parti delle credenziali da parte di terzi consentirebbe a questi ultimi l'utilizzo del sistema informatico e dei servizi erogati attraverso di esso. L'utente pertanto è tenuto a:
    - custodire con diligenza le proprie credenziali e non comunicarle ad altre persone (es.: non scrivere la password su carta o post-it lasciandoli sulla scrivania o attaccati al monitor; condividere con altri la propria password);
    - durante la digitazione della propria password, assicurarsi che nessuno stia osservando la tastiera con l'intenzione di memorizzarla.
11. L'utente è il solo ed unico responsabile della conservazione e della riservatezza della propria password e, conseguentemente, rimane il solo ed unico responsabile per tutti gli usi ad essa connessi o correlati, ivi compresi danni e conseguenze pregiudizievoli arrecati all'Ente e/o a terzi, siano dal medesimo utente autorizzati ovvero non autorizzati.
12. In caso di sottrazione della password o comunque in tutti i casi in cui si abbia fondato motivo di ritenere che possa essere compromessa la riservatezza della stessa o ne possa essere stato fatto un utilizzo da parte di terzi, l'utente dovrà provvedere al cambiamento della password. Qualora l'utente venga a conoscenza della password di altro, è tenuto a darne immediata notizia all'interessato affinché provveda a cambiarla.
13. Le password sono personali e riservate, si fa presente però che in caso di prolungata assenza o impedimento dell'utente, che renda indispensabile ed indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, il Dirigente del Servizio di appartenenza dell'utente, in qualità di fiduciario, può richiedere al Responsabile del Sistema Informativo Comunale che venga effettuato il reset della password dell'utente

stesso. Al termine del tempo strettamente necessario al recupero delle informazioni di lavoro protette da password, il suddetto Dirigente dovrà richiedere al Responsabile del Sistema Informativo Comunale un nuovo reset della password che, questa volta, sarà comunicato esclusivamente all'utente interessato.

Art. 9 – Utilizzo della rete del Comune di Rho

1. Per l'accesso alle risorse informatiche del Comune di Rho attraverso la rete locale, ciascun utente deve essere in possesso di credenziali di autenticazione secondo quanto previsto dall'articolo 8. È assolutamente proibito accedere alla rete e nei sistemi informatici utilizzando credenziali di altre persone.
2. Non è consentito accedere o collegarsi alla rete informatica comunale, con strumenti informatici (ad esempio personal computer esterni, router, switch, modem, ecc.) non in dotazione dell'Amministrazione stessa, fatto salvo quanto previsto al successivo articolo 11; è però consentito accedere dall'esterno alla posta elettronica di Ente e alla Intranet.
3. L'accesso alla rete garantisce a ciascun utente la disponibilità di condivisioni di rete (cartelle su server) nelle quali vanno inseriti e salvati i file di lavoro, organizzati per area/ufficio o per diversi criteri o per obiettivi specifici di lavoro. Sono infatti previste delle cartelle condivise su server/storage di dominio per la memorizzazione di dati e programmi accessibili ad utenti preventivamente dotati di credenziali.
4. L'organizzazione delle unità di rete prevede l'accesso degli utenti sia ad aree comuni - per la condivisione di file - che ad aree riservate per consentire un accesso limitato a pochi utenti autorizzati. È responsabilità dei dirigenti richiedere al personale del Sistema Informativo Comunale l'attivazione delle unità di rete agli utenti dei propri servizi.
5. Ferma restando l'accessibilità al dirigente e su richiesta dello stesso dirigente, è possibile creare cartelle ad accesso riservato al singolo utente.
6. Le cartelle presenti nei server sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non deve essere dislocato in queste unità. È vietato il salvataggio sulle cartelle di rete, ma anche sugli Strumenti informatici assegnati dall'Ente, di documenti non inerenti l'attività lavorativa, quali a titolo esemplificativo fotografie, video, musica, pratiche personali, sms, messaggi di

posta elettronica personali e quant'altro.

7. L'utente è tenuto a conservare tutti i dati di lavoro sulle condivisioni di rete, evitando di mantenere l'esclusività sugli stessi, anche al fine di favorire la sicurezza dei dati. Sulle unità di rete infatti vengono svolte regolari attività di controllo, amministrazione e back-up da parte del personale del Sistema Informativo Comunale.
8. I personal computer, tutti i dischi o altre unità di memorizzazione locali (es. disco C: interno personal computer; hard disk portatili) non sono soggette a salvataggio da parte del personale incaricato del Sistema Informativo Comunale. Tutte queste aree di memorizzazione non devono ospitare dati di interesse istituzionale, poiché non sono garantite la sicurezza e la protezione contro la eventuale perdita di dati. La responsabilità dei salvataggi dei dati ivi contenuti è a carico del singolo utente.
9. Risulta opportuno che, con regolare periodicità (almeno ogni sei mesi), ciascun utente provveda 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.
10. Il Comune di Rho rende noto che il personale incaricato che opera presso il servizio Sistema Informativo Comunale potrà accedere ai contenuti delle cartelle di rete, per le finalità e secondo le modalità indicate all'articolo 5 e 20. Ogni materiale personale rilevato a seguito di tali interventi viene rimosso secondo le regole previste dall'articolo 5 sopra citato, ferma ogni ulteriore responsabilità civile, penale e disciplinare.

Art. 10 – Utilizzo delle stazioni di lavoro

1. Gli utenti, come individuati all'art. 2, sono consapevoli che gli Strumenti forniti sono di proprietà del Comune di Rho e devono essere utilizzati esclusivamente per rendere la prestazione lavorativa. Ognuno è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione. Gli Strumenti, nonché le relative reti a cui è possibile accedere tramite gli stessi, sono domicilio informatico del Comune di Rho.
2. Il computer può essere affidato ad uso singolo o condiviso, sulla base della richiesta effettuata dal Responsabile del Servizio e tenuto conto della prevalenza delle funzioni che devono essere espletate.
3. 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 utente si deve quindi attenere alle seguenti regole di utilizzo degli Strumenti.

4. L'accesso agli Strumenti messi a disposizione dal Comune è protetto da password; per l'accesso devono essere utilizzati Username e password assegnate dal Sistema Informativo Comunale così come disciplinato dall'art. 8; a tal proposito si rammenta che esse sono strettamente personali e ciascun utente è tenuto a conservarli nella massima segretezza.
5. Il personal computer, notebook, tablet ed ogni altro hardware deve essere custodito con cura da parte degli assegnatari evitando ogni possibile forma di danneggiamento.
6. Le eventuali situazioni anomale, danneggiamenti, guasti e/o difetti di funzionamento dei dispositivi hardware e software devono essere tempestivamente segnalati al Sistema Informativo Comunale tramite richiesta di assistenza HelpDesk.
7. La configurazione dell'hardware e l'installazione del software nelle postazioni di lavoro e negli apparati di rete di proprietà del Comune è predisposta dal personale del Sistema Informativo Comunale o da personale esterno incaricato; l'utente è tenuto a non modificare la configurazione base hardware e software della postazione di lavoro assegnata e degli apparati di rete messi a disposizione.
8. Le richieste di installazione e aggiornamento di ulteriori applicativi rispetto a quelli di base devono essere preventivamente validate dal Responsabile del Sistema Informativo Comunale in ordine alle necessarie verifiche tecniche. Qualora venissero riscontrati programmi non autorizzati sulle postazioni di lavoro, anche se legali, questi verranno disinstallati secondo le modalità previste dall'articolo 5.
9. Nell'uso delle postazioni di lavoro è vietato:
    - alterare, disattivare o modificare le impostazioni di sicurezza e di riservatezza del sistema operativo, del software di navigazione, della posta elettronica e di ogni altro software installato sulle stazioni di lavoro;
    - l'uso di meccanismi o strumenti di qualsiasi natura atti ad eludere gli schemi di protezione da copia abusiva del software, a rivelare password, ad identificare eventuali vulnerabilità della sicurezza dei vari sistemi, a decrittare file crittografati o a compromettere la sicurezza della rete in qualsiasi modo;
    - utilizzare il personal computer per l'acquisizione, la duplicazione e/o la trasmissione illegale di opere protette da copyright;

- l'utilizzo di supporti di memoria (chiavi USB, CD, DVD o altri supporti) per il salvataggio di dati trattati tramite gli Strumenti comunali, salvo che il supporto utilizzato sia stato fornito dall'Ente; in tale caso, il supporto fornito può essere utilizzato esclusivamente per finalità lavorative;
- connettere al personal computer supporti e/o periferiche personali;
- installare modem che sfruttino il sistema di comunicazione telefonico per l'accesso a internet o a banche dati esterne.

10. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale del Sistema Informativo Comunale nel caso in cui siano rilevati virus ed adottando quanto previsto dall'articolo 18 relativo alle procedure di protezione antivirus.
11. L'installazione di componenti software in grado di danneggiare il sistema informatico o le informazioni in esso contenute costituisce illecito disciplinare e può costituire condotta sanzionata anche penalmente, ai sensi dell'art. 635 bis del codice penale (Danneggiamento di sistemi informatici e telematici).
12. Le informazioni archiviate sul personal computer locale devono essere esclusivamente quelle necessarie all'attività lavorativa assegnata. L'utente è comunque tenuto a conservare tutti i dati di lavoro sulle condivisioni di rete previste dall'articolo 9.
13. Costituisce buona regola la pulizia periodica degli archivi memorizzati sul proprio personal computer, con cancellazione dei file obsoleti o non più utili.
14. Non è consentita la consultazione, memorizzazione e diffusione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
15. E' obbligatorio utilizzare screen saver per la riservatezza dei dati visualizzati, che devono essere consoni all'ambiente lavorativo e che non contengano immagini offensive, irriguardose o fotografie in cui siano individuabili persone, situazioni e momenti soggetti a riservatezza e/o a tutela dell'immagine di persone. Analoghe indicazioni valgono per i Desktop.
16. Il personal computer deve essere spento al termine di ogni turno giornaliero di lavoro, prima di lasciare gli uffici, e comunque deve essere protetto nelle pause durante l'orario di lavoro. Pertanto, ogni qualvolta il dipendente si allontani o si assenti dalla postazione

di lavoro è tenuto a chiudere la sessione (Ctrl+Alt+Canc quindi "Blocca Computer"), oppure a rendere inaccessibile a terzi (ad esempio mediante l'utilizzo del salvaschermo dotato di password) la propria postazione di lavoro. E' evidente che lasciare incustodito un elaboratore 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.

17. Il Comune di Rho rende noto che il personale incaricato che opera presso il servizio Sistema Informativo Comunale potrà accedere ai contenuti delle singole postazioni personal computer, per le finalità e secondo le modalità indicate all'articolo 5 e 20.

Art. 11 – Utilizzo di hardware e software di proprietà personale

1. Al fine di proteggere l'integrità del sistema informatico, l'utente non può connettere postazioni di lavoro (personal computer, tablet, …) o apparati personali alle reti LAN e Wireless del Comune.
2. L'utente non può utilizzare software di proprietà personale. Tutto ciò comprende anche le applicazioni regolarmente acquistate e registrate a titolo personale dall'utente, i programmi shareware e/o freeware non resi disponibili dal Sistema Informativo Comunale, il software scaricato da Internet o proveniente da supporti magneto-ottici allegati a riviste e/o giornali o altro software ottenuto o posseduto a qualsiasi titolo.
3. Il personale esterno incaricato può connettersi alle reti del Comune con hardware di proprietà personale previa richiesta al Servizio Sistema Informativo Comunale. L'hardware sarà connesso alla rete e configurato a cura del Servizio Sistema Informativo Comunale o di personale esterno incaricato dal Servizio stesso. Nel caso in cui l'hardware non sia dotato di un software antivirus regolarmente aggiornato, sarà negato l'accesso alla rete.

Art. 12 – Utilizzo di dispositivi mobili

1. L'utente è responsabile dei dispositivi mobili quali notebook, cellulari, internet key, tablet assegnatigli e deve custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro. Se i dispositivi mobili sono condivisi da più persone, sarà compito del Responsabile del Servizio vigilare che siano usati in modo appropriato.
2. L'utilizzo di tali dispositivi è limitato all'utente o agli utenti assegnatari; è quindi vietato cederne l'uso, anche temporaneo, a terzi se non preventivamente autorizzato.
3. Ai dispositivi mobili si applicano le regole di utilizzo previste dall'articolo 10 per i

personal computer connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna. Tali disposizioni si applicano anche nei confronti di eventuali incaricati esterni.

4. L'installazione di programmi e "*app*", anche per tali dispositivi, dovrà essere effettuata a cura del Sistema Informativo Comunale, al fine di garantire il rispetto dei criteri di sicurezza informatica nell'uso della rete.
5. I dati dell'Ente di natura riservata, di norma, non possono essere registrati su dispositivi mobili; diversamente devono essere gestiti secondo le indicazioni del Sistema Informativo Comunale.
6. L'utilizzo di dispositivi mobili, all'esterno dei locali dell'Ente, deve essere oggetto di particolare cura ed attenzione da parte degli utenti perché questo utilizzo rappresenta una fonte di rischi particolarmente rilevante in termini di sicurezza, sia delle risorse in sé sia dei dati nelle stesse contenuti. Tali dispositivi, infatti, possono essere soggetti a smarrimento, furti, distruzione o compromissione dei dati, tentativi di frode e/o accesso non autorizzato ovvero essere "infettati" da virus o codice malevole. Peraltro un'eventuale contaminazione da virus informatici potrebbe diffondersi e ripercuotersi all'intera rete informatica dell'Amministrazione, una volta che tali dispositivi siano collegati direttamente alla rete interna.
7. E' necessario, pertanto, adottare ulteriori norme comportamentali nonché specifiche procedure, di seguito descritte, che gli utenti sono chiamati ad applicare in modo scrupoloso:
   - cifrare i dati (laddove possibile e previa analisi dei rischi/costi-benefici);
   - fare periodicamente delle copie di back-up dei dati e verificarle regolarmente;
   - autenticarsi, con frequenza almeno settimanale, alla rete dell'Ente per scaricare gli aggiornamenti forniti dall'Amministrazione;
   - mantenere abilitato l'antivirus;
   - non disabilitare le impostazioni di sicurezza originariamente impostate dall'Amministrazione;
   - evitare di accedere e navigare in siti *web* "pericolosi" per la sicurezza informatica, a prescindere dal fatto che ciò avvenga al di fuori dell'orario di lavoro;
   - non mantenere abilitati protocolli insicuri di comunicazione, come ad es. il

bluetooth, oltre il tempo strettamente necessario.

8. Il Comune di Rho rende noto che il personale incaricato che opera presso il servizio Sistema Informativo Comunale potrà accedere ai contenuti dei dispositivi mobili di cui al presente articolo, per le finalità e secondo le modalità indicate all'articolo 5 e 20.

Art. 13 – Posta elettronica

1. La gestione delle caselle di posta elettronica avviene in modo centralizzato su server sito nel data center del Comune in Piazza Visconti n. 24; il servizio è erogato secondo i massimi standard di sicurezza garantendo elevata disponibilità e possibilità di essere fruito sia dalla rete comunale che dall'esterno tramite personal computer, smartphone, tablet, ecc.
2. La finalità per cui è stata adottata la decisione di utilizzare il server dell'Ente per la gestione della posta elettronica è principalmente riconducibile alla determinante importanza delle comunicazioni per via telematica in un'attività come quella esercitata dall'Ente. Il server allocato all'interno della rete locale del Comune di Rho consente lo svolgimento continuativo del lavoro anche quando si verificano malfunzionamenti della linea internet; infatti in tali circostanze ogni utente può continuare a lavorare in modalità offline, anche accedendo alla propria corrispondenza pregressa.
3. Le caselle di posta elettronica rilasciate sono di due tipi:
   - casella di posta elettronica individuale, assegnata ad un utente interno del tipo *nome.cognome@comune.rho.mi.it*;
   - casella di posta elettronica collettiva, riconducibile ad un'unità operativa o ad un gruppo funzionale di utenti che operano all'interno di una stessa unità operativa o in più unità operative del tipo *unità.operativa@comune.rho.mi.it*.
4. Gli indirizzi di posta elettronica di Ente assegnati ai dipendenti vengono configurati all'interno del server comunale. Ogni casella di posta elettronica è contenuta in un database, residente sul server, il quale raccoglie e conserva tutta la corrispondenza in entrata e in uscita dalla casella medesima, fino a cancellazione da parte del titolare dell'indirizzo di posta elettronica.
5. Al singolo indirizzo di posta elettronica, può avere accesso solo l'interessato, intestatario dell'indirizzo stesso, fatto salvo quanto previsto dagli articoli 5 e 20.
6. Si informa che i messaggi di posta elettronica cancellati dagli utenti vengono

"conservati" per 7 giorni sul server di posta dell'Ente a tutela degli utenti medesimi in caso di cancellazioni involontarie.

7. Il server di posta elettronica, e conseguentemente tutta la corrispondenza in entrata e in uscita dalle caselle di posta elettronica, viene quotidianamente soggetto a backup e la copia di backup viene conservata per 30 giorni.
8. Per motivi di gestione, sicurezza e di controllo delle performance del sistema, è installato un sistema centralizzato Antivirus/malware e Antispam. I messaggi in entrata vengono quindi sistematicamente analizzati alla ricerca di virus, malware e per l'eliminazione dello spam. I messaggi che dovessero contenere virus e malware vengono automaticamente eliminati dal sistema, lo stesso per i messaggi che dal sistema di monitoraggio sono ritenuti con alta probabilità di essere spam; i messaggi che hanno una media probabilità di essere spam vengono invece conservati per 30 giorni per essere eventualmente recuperati su richiesta dell'utente.
9. Sempre per motivi di gestione, sicurezza e di controllo delle performance, il sistema di gestione della posta elettronica provvede alla tracciatura su file di log della corrispondenza in entrata e in uscita; sul punto si rinvia a quanto previsto all'articolo 20 e 21.
10. Al fine di garantire la funzionalità del servizio di posta elettronica di Ente e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, in caso di assenza prolungata programmata (ad es. per ferie o comando presso altro ente) l'utente è tenuto all'attivazione del sistema di risposta automatica ai messaggi di posta elettronica ricevuta indicando, nel messaggio di accompagnamento, le coordinate di un collega o della struttura di riferimento che può essere contattata.
11. In caso di assenza non programmata (ad es. per malattia) la procedura potrà essere attivata a cura del Sistema Informativo Comunale, su richiesta del Dirigente del Servizio di appartenenza dell'utente in qualità di fiduciario, dandone informazione all'utente appena possibile.
12. In caso di assenza improvvisa o prolungata dell'utente e per obiettive necessità di ufficio il Dirigente di riferimento dell'utente assente può richiedere al Sistema Informativo Comunale il reset della password come previsto dall'articolo 8 – comma 12.
13. In caso di cessazione dell'attività presso il Comune di Rho, la casella nominativa di posta

elettronica sarà prontamente disattivata come previsto all'articolo 7. I messaggi di posta elettronica dei dipendenti sono conservati sino a 60 giorni dopo la cessazione del rapporto di lavoro. Se per esigenze lavorative sorgesse la necessità di accedere al contenuto di tale casella di posta, il Dirigente del Servizio di appartenenza dell'utente, in qualità di fiduciario, potrà inoltrare motivata richiesta al Responsabile del Sistema Informativo Comunale e dell'accesso dovrà essere informato, possibilmente preventivamente, l'intestatario dell'indirizzo di posta elettronica.

14. Fermi restando i limiti generali di accesso da parte del Datore di lavoro alla posta elettronica messa a disposizione del lavoratore, in caso di controllo su base individuale e nominativa, visti i divieti previsti dal presente disciplinare di utilizzo della posta elettronica per motivi diversi da quelli strettamente legati all'attività lavorativa, l'Amministrazione presuppone che si tratti di Posta Elettronica professionale. Pertanto tale accesso non configura da parte dell'Ente una violazione della normativa in materia di privacy.

Art. 14 – Utilizzo della posta elettronica

1. La casella di posta elettronica individuale assegnata ad un utente, nonché quelle collettive cui eventualmente quest'ultimo abbia accesso, sono uno strumento di lavoro ed il loro utilizzo è consentito solo per finalità connesse allo svolgimento della attività lavorativa. L'utente è responsabile del corretto utilizzo delle caselle di posta elettronica a cui ha accesso.
2. È raccomandato l'utilizzo delle caselle di posta elettronica associate a ciascuna unità organizzativa, ufficio o gruppo di lavoro qualora le comunicazioni siano di interesse collettivo: questo per evitare che degli utenti singoli mantengano l'esclusività su dati dell'Ente.
3. L'accesso al servizio di posta elettronica da parte di un utente avviene mediante le credenziali di autenticazione (user-id e password) di accesso al sistema informatico, rilasciate secondo le modalità individuate all'articolo 8. L'utente è informato del fatto che la conoscenza delle credenziali di autenticazione da parte di terzi consentirebbe a questi ultimi l'utilizzo del servizio di posta elettronica in nome dell'utente medesimo e l'accesso alla sua corrispondenza di posta elettronica. L'articolo 8 definisce le modalità per la corretta conservazione, responsabilità ed uso delle credenziali.

4. E' vietato utilizzare la user-id/password di un altro utente per accedere in sua assenza alla sua posta elettronica.
5. Nell'utilizzo della posta elettronica di Ente l'utente è tenuto ad osservare alcune norme di comportamento di seguito indicate.
6. L'utente è tenuto a leggere quotidianamente i messaggi di posta elettronica di sua competenza.
7. I messaggi devono essere di solo testo, evitando ogni formattazione e inserzione di immagini/motivi decorativi. È buona norma inviare messaggi sintetici che descrivano in modo chiaro la questione; indicare sempre chiaramente l'oggetto, in modo tale che il destinatario possa immediatamente individuare l'argomento del messaggio ricevuto, facilitandone la successiva ricerca per parole chiave.
8. È consentito inviare messaggi di posta elettronica a indirizzi plurimi numerosi (decine di destinatari) solo in casi motivati da esigenze di servizio.
9. L'invio di un messaggio di posta elettronica al gruppo di distribuzione denominato "Tutti", comportando l'invio del messaggio a tutti i dipendenti o collaboratori dell'Ente, è consentito solo se richiesto da esigenze di servizio e previa autorizzazione del Dirigente di riferimento.
10. Le caselle di posta hanno una dimensione predefinita e non estendibile, occorre pertanto mantenere in ordine la propria casella di posta badando a ripulirla con regolarità, cancellando documenti inutili e soprattutto allegati ingombranti che potranno essere eventualmente salvati sulla rete.
11. Nel caso fosse necessario inviare allegati "pesanti" (fino a 20 MB) è opportuno ricorrere prima alla compressione dei file originali in un archivio di formato zip o equivalenti. Nel caso di allegati ancora più voluminosi è necessario rivolgersi al Sistema informativo Comunale.
12. Ogni comunicazione via posta elettronica con soggetti esterni od interni all'Amministrazione deve avvenire mediante l'utilizzo del sistema di posta elettronica comunale, per garantire i necessari livelli di sicurezza e riservatezza. Non è autorizzato l'utilizzo per fini istituzionali di indirizzi di posta elettronica personali privati al di fuori del dominio dell'nte.
13. L'invio e la ricezione di messaggi di posta elettronica è consentito per lo scambio di

comunicazioni e documenti utili all'esercizio della propria attività lavorativa; tale modalità va utilizzata ordinariamente; qualora si necessiti di attestazione ufficiale è invece necessario utilizzare le caselle PEC integrate nel sistema di Protocollo Informatico attivo nell'Ente.

14. Tutti i dipendenti e collaboratori, anche nell'ambito dell'utilizzo della posta elettronica di Ente, sono comunque tenuti a prestare particolare cautela nel trattamento dei dati personali e sensibili ai quali sono preposti nel pieno rispetto della normativa vigente in materia. Gli stessi si impegnano ad adottare ogni precauzione necessaria per evitare ed escludere il trattamento, la comunicazione e/o la diffusione di dati personali e/o sensibili non necessaria per l'espletamento delle proprie competenze istituzionali.
15. 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 decrittazione deve essere comunicata al destinatario attraverso un canale diverso dalla posta elettronica (ad esempio per lettera o per telefono) e mai assieme ai dati crittati.
16. È vietato l'invio automatico di messaggi di posta elettronica al proprio indirizzo privato, attivando per esempio un "inoltro" automatico dei messaggi di posta elettronica in entrata o in uscita.
17. Non è consentita l'iscrizione a mailing-list non legate ad esigenze professionali.
18. Prima di iscriversi a mailing-list o newsletter legate ad esigenze professionali occorre verificare anticipatamente l'affidabilità del sito che offre il servizio.
19. Non è consentito l'invio di lettere a catena (es. catena di S. Antonio); ciò include lettere per nobili cause vere o presunte; se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al personale del Sistema Informativo Comunale; non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.
20. Non è consentito l'utilizzo di programmi di sicurezza e/o crittografia non previsti esplicitamente dalle procedure di sicurezza messe in atto dal Servizio Sistema Informativo Comunale.
21. Non è consentito utilizzare la posta elettronica di Ente per esprimere punti di vista ufficiali del Comune salvo espressa autorizzazione, né per diffondere opinioni personali.

22. È fatto divieto, in ogni caso, di immettere in rete informazioni che possano presentare forme o contenuti di carattere pornografico, pedofilo, molesto, osceno, blasfemo, fraudolento/illegale, attinente a gioco d'azzardo, razzista, diffamatorio o offensivo; il predetto divieto riguarda tanto il contenuto quanto gli allegati dei messaggi di Posta.
23. Allo scopo di garantire sicurezza alla rete, occorre 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, eccetera. 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 il Sistema Informativo Comunale per una valutazione dei singoli casi.
24. Eventuali anomalie nell'invio e ricezione dei messaggi di posta elettronica devono essere segnalate al Sistema Informativo Comunale mediante help desk.
25. Al momento della conclusione del rapporto di lavoro dovuto a qualunque causa, si applicano le disposizioni di cui al precedente art. 7 del presente Regolamento.

Art. 15 – Protocollo informatico

1. In conformità alla normativa in materia di amministrazione digitale il Comune di Rho si è dotata di un software di gestione documentale e Protocollo informatico, secondo le modalità disciplinate nel relativo Manuale adottato dall'Amministrazione comunale a cui si rinvia. L'accesso al sistema di Protocollo informatico avviene mediante l'utilizzo di credenziali nel rispetto della procedura degli accessi descritta nel precedente articolo 8. La configurazione dei gruppi di accesso al sistema documentale è in carico al Responsabile del Protocollo, il quale li attribuisce sulla base di una procedura condivisa con il dirigente dell'ufficio/struttura/servizio.
2. Si evidenzia che tutti i documenti dai quali possano nascere diritti, doveri o legittime aspettative di terzi, a eccezione di quelli sottratti alla registrazione, devono essere protocollati. Il registro di protocollo, infatti, da un punto di vista giuridico è un atto pubblico destinato a far fede della data di protocollazione dei documenti trattati da una pubblica amministrazione, indipendentemente dalla regolarità del documento stesso, ed è idoneo a produrre effetti giuridici a favore o a danno delle parti. I singoli documenti e l'archivio del comune di Rho, in quanto ente pubblico, sono beni culturali, assoggettati

al regime proprio del demanio pubblico e quindi sono inalienabili.

3. I documenti che transitano dal protocollo informatico sono archiviati con modalità idonee a garantire le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità prescritte dalla disciplina di settore applicabile. I sistemi di posta elettronica invece, per loro stessa natura, non consentono di assicurare tali caratteristiche.

Art. 16 – Navigazione in Internet

1. La stazione di lavoro assegnata al singolo utente ed abilitata alla navigazione in Internet costituisce uno strumento di proprietà del Comune utilizzabile esclusivamente per lo svolgimento dell'attività lavorativa.
2. Durante l'orario di lavoro, i dipendenti possono accedere per finalità personali a siti di informazione (giornali e quotidiani) e/o di altro genere, purché per un periodo di tempo assai limitato e tale da non pregiudicare il disbrigo assiduo e diligente delle mansioni assegnate. Non è invece consentito effettuare trading on line con istituti di credito.
3. L'accesso alla rete internet è consentito con policy di sicurezza debitamente implementate e aggiornate che impediscono l'accesso a siti a carattere pornografico, di violenza, razzista, ecc. Tuttavia il sistema di filtro non garantisce l'interdizione al 100% di determinati siti, pertanto l'utente si deve attenere comunque a quanto indicato al successivo punto 7.
4. Nel caso in cui, per ragioni di servizio, si necessiti di una navigazione libera dai suddetti filtri, è necessario richiedere lo sblocco mediante una richiesta formale indirizzata al dirigente del Sistema Informativo Comunale, ed in copia al Titolare del Trattamento/Sindaco, nella quale siano indicati chiaramente: motivo della richiesta, utente, postazione da cui effettuare la navigazione libera e intervallo di tempo richiesto per completare l'attività.
5. Il Comune di Rho si riserva di bloccare l'accesso a siti "a rischio" anche 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 dell'Ente, contattare il Sistema Informativo Comunale per uno sblocco selettivo.

6. 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.
7. Ciascun utente si deve attenere alle seguenti regole di utilizzo della rete Internet e dei relativi servizi. Sono esplicitamente vietati/e:

- l'uso e la navigazione su siti web che possano presentare forme o contenuti di carattere pornografico, osceno, blasfemo, razzista, diffamatorio o offensivo;
- l'upload o il download di software gratuiti (freeware e shareware), nonché l'utilizzo di documenti provenienti da siti web, se non strettamente attinenti all'attività lavorativa (es.: filmati e musica) e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà essere a tal fine contattato il personale del Sistema Informativo Comunale);
- la condivisione via Internet di file, anche di tipo audio/video o immagini, non legati alle attività professionali;
- lo svolgimento di qualsiasi attività intesa ad eludere o ingannare i sistemi di controllo di accesso e/o sicurezza di qualsiasi server interno o pubblico;
- la partecipazione a forum, chat line, bacheche elettroniche e social network (ad esempio Facebook e similari), fatti salvi motivi istituzionali o professionali;
- la consultazione delle banche dati a pagamento per finalità non pertinenti ai propri doveri d'ufficio, pur essendo autorizzati all'accesso;
- lo scambio di materiale protetto dalla normativa vigente in tema di tutela del diritto d'autore e utilizzare sistemi di scambio dati/informazioni con tecnologie "peer to peer" (da utente a utente);
- l'utilizzo del servizio internet per sollecitare o fare proseliti per finalità commerciali, a beneficio di organizzazioni esterne, per catene di lettere ovvero per altre finalità estranee all'attività dell'Ente;
- l'utilizzo di strumenti di file sharing di qualsiasi natura, esclusi quelli eventualmente resi disponibili dal Sistema Informativo Comunale.

Art. 17 – Utilizzo di telefoni, fax, stampanti, scanner e fotocopiatrici

1. Il telefono fornito dall'Ente (fisso e/o cellulare) è uno strumento di lavoro e a fini privacy deve essere impostato un codice di accesso per l'utilizzo. L'uso di tale telefono è consentito esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali mediante utilizzo del telefono di ente è consentito solo nel caso di necessità ed urgenza.
2. Per gli smartphone è vietata l'installazione e l'utilizzo di applicazioni (o altresì denominate "app") diverse da quelle autorizzate dal Sistema Informativo Comunale.
3. In caso di smarrimento o furto del cellulare di servizio si applicano le disposizioni di cui al precedente art. 6 del presente Regolamento.
4. L'utilizzo del proprio cellulare personale durante l'orario di lavoro è consentito laddove ricorrano ragioni di necessità e/o urgenza. L'utilizzo deve essere comunque improntato a criteri di buona fede e correttezza e non può in alcun caso pregiudicare il disbrigo assiduo e diligente delle mansioni assegnate.
5. È vietato l'utilizzo di strumenti forniti dall'Ente quali fax, stampanti, scanner e fotocopiatrici per fini personali. In caso di necessità e urgenza, gli utenti possono utilizzare tali beni per motivi non attinenti l'attività lavorativa e, comunque, non in modo ripetuto o per periodi di tempo prolungati.
6. Per quanto concerne l'uso delle stampanti, al fine di ridurre l'utilizzo di carta e materiali di consumo (toner ed altri consumabili), gli utenti sono tenuti a:
   - stampare documenti solo se strettamente necessari per lo svolgimento delle proprie funzioni operative;
   - prediligere le stampanti di rete condivise, rispetto a quelle locali/personali eventualmente collegate;
   - prediligere la stampa in bianco/nero e fronte/retro.
7. Nel caso in cui si rendesse necessaria la stampa di informazioni riservate o comunque contenenti dati personali, le stampe dovranno essere protette da password. Qualora il dispositivo utilizzato non prevedesse questa funzione, l'utente dovrà presidiare la stampante per evitare la possibile perdita o divulgazione di tali informazioni a persone terze non autorizzate.

8. Il controllo sul corretto utilizzo degli strumenti in parola è affidato al Responsabile del Servizio a cui detti strumenti sono stati assegnati.
9. Il Comune di Rho rende noto che il personale incaricato che opera presso il servizio Sistema Informativo Comunale potrà accedere ai contenuti degli strumenti aziendali di cui al presente articolo, per le finalità e secondo le modalità indicate agli articoli 5 e 20.

Art. 18 – Protezione antivirus

1. Al fine di proteggere l'integrità del sistema informatico, il Comune di Rho si è dotato di:
   - apparati di sicurezza perimetrale che possono limitare la visibilità di siti web o servizi esterni e prevedere l'analisi del traffico da/verso Internet;
   - Sistema Antivirus centralizzato che protegge tutte le macchine in uso presso i vari Servizi ed Uffici;
   - Sistema Antispam centralizzato per l'analisi della posta elettronica.
2. L'antivirus è installato su ogni postazione di lavoro a cura del Sistema Informativo Comunale. E' fatto assoluto divieto a ciascun utente di modificare le impostazioni del software antivirus. L'aggiornamento avviene in maniera automatica, in caso di errori si invita ad avvisare il personale del Sistema Informativo Comunale tramite Help Desk.
3. Nel caso in cui il software antivirus rilevi la presenza di un virus che non è riuscito a ripulire, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer e segnalare prontamente l'accaduto al personale del Sistema Informativo Comunale tramite Help Desk. Stessa cosa qualora noti comportamenti anomali quali esecuzione automatica di programmi, alterazione di file, e così via.
4. L'utente è tenuto ad osservare tutte le prescrizioni fornite dal Sistema Informativo Comunale al fine di evitare infezioni e installazione di software malevolo, in particolare:
   - ogni dispositivo di provenienza esterna all'Ente dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale del Sistema Informativo Comunale;
   - non aprire allegati o visitare link contenuti in messaggi di posta elettronica di dubbia provenienza; nel caso si abbiano dubbi in merito contattare preventivamente il Sistema Informativo Comunale.

Art. 19 – Utilizzo di social media

1. Il presente articolo deve essere osservato dagli utenti sia che utilizzino dispositivi messi a disposizione dall'Ente, sia che utilizzino propri dispositivi, sia che partecipino ai social media a titolo personale, sia che lo facciano per finalità professionali, come dipendenti/collaboratori del Comune di Rho.
2. Fermo restando il pieno ed inderogabile diritto della persona alla libertà di espressione e al libero scambio di idee ed opinioni, il Comune di Rho ritiene infatti opportuno indicare agli utenti alcune regole comportamentali di seguito specificate, al fine di tutelare tanto la propria immagine ed il patrimonio dell'Ente, anche immateriale, quanto i propri collaboratori, i propri clienti e fornitori, oltre che gli stessi utenti utilizzatori dei social media. Resta fermo che viene vietata la partecipazione per fini non lavorativi agli stessi social media durante l'orario di lavoro.
3. L'utilizzo a fini lavorativi dei social media – quali Facebook™, Twitter™, Linkedin™, dei blog e dei forum, anche professionali – verrà gestito ed organizzato esclusivamente dal Comune di Rho attraverso specifiche direttive ed istruzioni operative al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli utenti.
4. La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni istituzionali considerate dal Comune 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.
5. Ogni comunicazione e divulgazione di contenuti, inoltre, dovrà essere effettuata nel pieno rispetto dei diritti di proprietà industriale e dei diritti d'autore, sia di terzi che del Comune. Il dipendente/collaboratore, nelle proprie comunicazioni, non potrà pubblicare disegni, modelli od altro connesso ai citati diritti. Ogni deroga a quanto sopra disposto potrà peraltro avvenire solo previa specifica autorizzazione del Sindaco quale Titolare del trattamento.
6. Il dipendente/collaboratore 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, se non con il preventivo consenso del Dirigente di riferimento.

7. L'utente risponde personalmente dei propri comportamenti e deve astenersi dal porre in essere, nei confronti in genere di terzi e specificatamente verso l'Ente, i colleghi ed i fornitori, attività che possano essere penalmente o civilmente rilevanti; a titolo esemplificativo, sono quindi vietati comportamenti ingiuriosi, diffamatori e denigratori, discriminatori o che configurano molestie. In tal senso, è vivamente auspicato da parte di tutti un comportamento civile e sobrio, in particolar modo in qualunque occasione in cui l'espressione o il contesto in cui essa avviene possa essere collegata all'ambito lavorativo.
8. Infine, in via generale ed ove non autorizzato in senso diverso dal proprio Dirigente, nell'uso dei social media, l'utente 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 al Comune di Rho.

Art. 20 – Controlli

1. Per motivi di gestione, sicurezza e di controllo delle performance del sistema, l'Antispam della posta elettronica provvede alla tracciatura su file di log della corrispondenza in entrata e in uscita, secondo la normativa vigente, che prevede esclusivamente la registrazione dell'oggetto, del mittente e del destinatario.
2. Anche l'uso degli Strumenti Informatici del Comune può lasciare traccia delle informazioni sul relativo uso tramite file di log, come chiarito all'articolo 5.
3. Il Comune di Rho effettua controlli sull'uso degli strumenti elettronici da parte degli utenti tramite consultazione dei file di log, in via eccezionale, in relazione e limitatamente a:
   - particolari esigenze tecniche o di sicurezza
   - indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria
   - obbligo di custodire o di consegnare dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.
4. Qualora le misure tecniche preventive non fossero sufficienti ad evitare eventi dannosi o

situazioni di pericolo, il Comune effettua con gradualità, nel rispetto dei principi di pertinenza e non eccedenza, le verifiche di eventuali situazioni anomale attraverso le seguenti fasi:

- analisi aggregata del traffico di rete riferito all'intera struttura lavorativa o a sue aree (reparto, servizio, ecc.) e rilevazione della tipologia di utilizzo (messaggi posta elettronica, file audio, accesso a risorse estranee alle mansioni);
- emanazione di un avviso generalizzato relativo ad un riscontrato utilizzo anomalo degli strumenti aziendali, con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite; il richiamo all'osservanza delle regole può essere circoscritto agli operatori afferenti al settore in cui è stata rilevata l'anomalia;
- in caso di successivo permanere di una situazione non conforme, é possibile effettuare controlli circoscritti su singole postazioni di lavoro.

5. L'Amministrazione si riserva anche di effettuare controlli per verificare il rispetto del presente disciplinare.
6. È sempre fatta salva l'ipotesi dell'attivazione di controlli, anche individualizzati, che trovino giustificazione nella necessità di rispondere ad eventuali richieste di organi di polizia e/o su segnalazione dell'autorità giudiziaria o nella presenza di sospetti relativamente all'esistenza di condotte improprie nell'uso delle apparecchiature (cd. controlli difensivi).
7. Con la stessa gradualità vengono effettuati controlli anche sull'occupazione dello spazio di memorizzazione sui server di ente attraverso le seguenti fasi:
   - analisi aggregata dei dati memorizzati sui server a livello di intera struttura lavorativa (reparto, servizio, ecc.) e rilevazione della tipologia di utilizzo (file audio, file video, immagini, software) e relativa pertinenza con l'attività lavorativa;
   - emanazione di un avviso generalizzato relativo ad un riscontrato utilizzo anomalo degli strumenti aziendali, con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite; il richiamo all'osservanza delle regole può essere circoscritto agli operatori afferenti il settore in cui è stata rilevata l'anomalia;
   - in caso di successivo permanere di una situazione non conforme, è possibile procedere con un analisi puntuale e, previo avviso all'utente interessato, ad una eventuale eliminazione del materiale non conforme.

8. Oltre a ciò, l'Ente si riserva di effettuare specifici controlli sui software caricati sui personal computer utilizzati dai dipendenti al fine di verificarne la regolarità sotto il profilo delle autorizzazioni e delle licenze, nonché, in generale, la conformità degli stessi alla normativa vigente e, in particolare, alle disposizioni in materia di proprietà intellettuale. Il personale del Sistema Informativo Comunale, in caso di identificazione di file o applicazioni in genere pericolose per la sicurezza della rete e/o dei singoli personal computer, potrà procedere alla rimozione degli stessi, previa comunicazione all'utente interessato salvo casi di urgenza.

Art. 21 – Conservazione dei dati

1. In applicazione ai principi di diritto di accesso, legittimità, proporzionalità, sicurezza ed accuratezza e conservazione dei dati, i file di log di cui al comma 1 del precedente articolo 20 vengono conservati non oltre 50 giorni, ossia il tempo indispensabile per il corretto perseguimento delle finalità di sicurezza dell'Ente. I file di log generati dall'uso di Strumenti Informatici quale il personal computer, di cui al comma 2 del citato articolo 20, devono essere nel caso cancellati a cura dell'utente.
2. Si ricorda che i messaggi di posta elettronica cancellati dagli utenti rimangono "conservati" per sette giorni sul server di posta dell'Ente a tutela degli utenti in caso di cancellazioni involontarie. Il server di posta elettronica, e conseguentemente tutta la corrispondenza in entrata e in uscita dalle caselle di posta elettronica, viene quotidianamente soggetto a backup e la copia di backup viene conservata per 30 giorni.
3. I messaggi in entrata che dal sistema antispam sono ritenuti con una media probabilità di essere spam vengono conservati per 30 giorni per essere eventualmente recuperati su richiesta dell'utente.
4. I predetti termini di conservazione, in via eccezionale, possono essere prolungati in relazione e limitatamente a:
   - particolari esigenze tecniche o di sicurezza
   - indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria
   - obbligo di custodire o di consegnare dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.
5. In caso di attivazione di controlli, anche individualizzati, che trovino giustificazione

nella necessità di rispondere ad eventuali richieste di organi di polizia e/o su segnalazione dell'autorità giudiziaria o nella presenza di sospetti relativamente all'esistenza di condotte improprie nell'uso delle apparecchiature (cd. controlli difensivi), i dati verranno conservati per il tempo strettamente necessario considerata la motivazione che è alla base del trattamento.

Art. 22 – Informativa in materia di Privacy

1. PREMESSA: gli Strumenti tecnologici considerati nel presente Regolamento costituiscono tutti strumenti utilizzati dal lavoratore esclusivamente per rendere la prestazione lavorativa; le informazioni raccolte sulla base di quanto indicato nel presente Regolamento possono essere utilizzate a tutti i fini connessi al rapporto di lavoro, visto che lo stesso costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Regolamento Europeo n. 679/16 "General Data Protection".

   TITOLARE E OGGETTO DEL TRATTAMENTO: ai sensi e per gli effetti dell'art. 13 del Regolamento (UE) 2016/679, si informa che il Comune di Rho, in persona del Sindaco e legale rappresentante, è TITOLARE del trattamento. Il trattamento ha per oggetto i dati personali, sensibili e giudiziari di cui gli operatori del Sistema Informativo Comunale o altro personale tecnico incaricato dal Titolare, vengono a conoscenza durante le attività previste dal presente disciplinare, in particolare le attività di cui all'art. 5 e all'art. 20.

   FINALITÀ: la finalità del trattamento è la gestione, sicurezza e controllo delle performance del sistema informatico comunale, nonché la verifica del corretto utilizzo degli Strumenti informatici nel rapporto di lavoro.

   MODALITA' DEL TRATTAMENTO: gli operatori del Sistema Informativo Comunale, o personale tecnico esterno autorizzato, effettueranno il trattamento dei dati con strumenti informatici; specifiche misure di sicurezza sono osservate per prevenire la perdita dei dati, usi illeciti o non corretti ed accessi non autorizzati.

   COMUNICAZIONE DEI DATI: il trattamento di verifica di norma è effettuato con gradualità e per aree aggregate per cui i dati non vengono comunicati con riferimento al trattamento del singolo lavoratore; i dati relativi ai singoli lavoratori potranno essere comunicati a Organismi di vigilanza, Autorità giudiziarie, nonché a quei soggetti ai quali la comunicazione sia obbligatoria per legge; la comunicazione, nel caso in cui si accerti

un uso indebito della singola postazione, sarà altresì data al Dirigente al quale appartiene il dipendente, per la valutazione del caso sotto il profilo disciplinare.

TRASFERIMENTO DATI: la gestione e la conservazione dei dati personali avverrà in Europa, su server ubicati in Italia del Titolare e/o di società terze incaricate e debitamente nominate quali Responsabili del trattamento. Resta in ogni caso inteso che il Titolare, ove si rendesse necessario, avrà facoltà di spostare i server anche extra-UE. In tal caso, il Titolare assicura sin d'ora che il trasferimento dei dati extra-UE avverrà in conformità alle disposizioni di legge applicabili, previa stipula delle clausole contrattuali standard previste dalla Commissione Europea.

DIRITTI DELL'INTERESSATO: ogni utente del sistema informatico del Comune di Rho, nella Sua qualità di interessato, ha il diritto di accesso di cui all'art. 15 del Regolamento (UE) 2016/679, ha altresì, ove applicabili, i diritti di cui agli artt. 16-21 del Regolamento (UE) 2016/679 (Diritto di rettifica, diritto all'oblio, diritto di limitazione di trattamento, diritto alla portabilità dei dati, diritto di opposizione), nonché il diritto di reclamo all'Autorità Garante.

MODALITÀ DI ESERCIZIO DEI DIRITTI: per l'esercizio dei diritti sopra descritti è possibile inviare un messaggio all'indirizzo di posta elettronica segreteria.sindaco@comune.rho.mi.it, a tale richiesta sarà fornito idoneo riscontro secondo le tempistiche previste dal Regolamento (UE) 2016/679; il Responsabile protezione dati personali (RDP) potrà essere contattato al seguente indirizzo di posta elettronica rdp.privacy@comune.rho.mi.it.

2. 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 loro utilizzo come strumenti per il controllo a distanza dell'attività dei lavoratori; peraltro, lì dove l'adozione di tali apparati risultasse necessaria per finalità altre di sicurezza del lavoro e/o di tutela del patrimonio aziendale, ad esempio esigenze organizzative e produttive, il Comune di Rho provvederà conformemente a quanto disposto dall'art.4, comma primo, della Legge n.300/1970 (Statuto dei lavoratori), dandone anche opportuna informazione agli utenti stessi.

Art. 23 – Sanzioni

1. Il mancato rispetto o la violazione delle regole contenute nel presente Regolamento è perseguibile con provvedimenti disciplinari, salve le azioni civili e penali consentite.
2. L'utente è considerato direttamente responsabile per il danneggiamento della strumentazione informatica aziendale e delle relative infrastrutture, causato dall'uso improprio della stessa, salvo il diritto dell'Ente di chiedere l'ulteriore risarcimento del danno. È altresì responsabile del trattamento illecito dei dati personali causato dall'uso improprio delle credenziali di accesso di cui all'articolo 8.

Art. 24 – Disposizioni finali

1. Per quanto non espressamente previsto dal presente Regolamento, si rinvia alle disposizioni generali vigenti in materia.

Art. 25 – Entrata in vigore e pubblicità.

1. Il presente Disciplinare entra in vigore a decorrere dalla data di esecutività della deliberazione di approvazione e sostituisce integralmente tutti i precedenti atti adottati in materia.
2. Del presente Disciplinare sarà fornita pubblicità e diffusione mediante pubblicazione nell'Intranet aziendale.
3. Tale pubblicazione assolve all'obbligo di informazione di cui all'art. 4, comma terzo, della Legge n.300/1970 (Statuto dei lavoratori) e dell'art. 13 del Regolamento Europeo n. 679/16.