INDICAZIONI OPERATIVE SUI DOVERI DI COMPORTAMENTO NELLA DETENZIONE ED UTILIZZO DELLE RISORSE TECNOLOGICHE

Sommario

Premessa

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete tramite i personal computer, espone il Comune a possibili rischi di natura sia patrimoniale sia penale, con conseguenti problemi alla sicurezza e all'immagine dell'Ente stesso.

L'utilizzo delle risorse informatiche e telematiche dell'Ente deve sempre ispirarsi al principio di diligenza e correttezza, atteggiamenti questi destinati a sorreggere ogni atto o comportamento posto in essere nell'ambito del rapporto di lavoro.

Il personal computer, i relativi programmi, applicazioni, dati, documenti ed archivi affidati in uso al personale (dipendente e non) sono strumenti di lavoro di proprietà dell'Ente. Tutto quanto messo a disposizione, ricevuto, rilasciato e comunque memorizzato sul posto di lavoro e sui mezzi di comunicazione è, e rimane, di proprietà dell'Ente.

Il Garante della Privacy è intervenuto sul tema dell'utilizzo nel rapporto di lavoro della posta elettronica e della rete Internet con il provvedimento n. 13 del 1° marzo 2007, indicando ai datori di lavoro le linee guida da adottare a garanzia degli interessi del personale dipendente, garantendo l'adozione delle misure di sicurezza idonee ad assicurare la disponibilità e l'integrità dei sistemi informativi e dei dati.

Inoltre lo Statuto dei Lavoratori (L.300/70) all'art. 4 prevede che

> "*Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna.*"

Quanto indicato nel presente disciplinare rappresenta istruzioni operative che permettono di effettuare una gestione dei sistemi a garanzia della sicurezza delle informazioni in conformità a quanto richiesto dal Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (da ora in poi GDPR).

Scopo e campo di applicazione

Le presenti indicazioni operative si applicano a tutti i lavoratori dipendenti del Comune di Garbagnate Milanese, nonché a tutto il personale che, a qualsiasi titolo, (amministratori, consulenti, stagisti…), - quindi a prescindere dal tipo di rapporto di lavoro e utilizzazione con lo stesso intercorrente - presti la propria attività, anche saltuaria e/o consulenziale, presso le sedi del Comune di Garbagnate Milanese e che, per ragioni connesse all'espletamento del proprio lavoro, risulti comunque autorizzato e abilitato all'uso, anche solo occasionale e/o temporaneo, delle risorse informatiche dell'Amministrazione.

Alla luce di quanto premesso, il Comune di Garbagnate Milanese adotta il presente disciplinare interno al fine di:

- evitare comportamenti inconsapevoli che possano innescare problemi o minacce alla sicurezza nel trattamento dei dati;
- informare il personale di quali sono le misure di tipo organizzativo e tecnologico adottate dall'Ente per la sicurezza dei dati;

- informare il personale su come vengono trattati i dati relativi all'uso dei mezzi informatici per la tutela dei lavoratori.

Questo documento non si riferisce solamente all'utilizzo di internet o della rete locale, ma si riferisce a tutto l'insieme delle risorse informatiche, di calcolo, di comunicazione, elettroniche, audiovisive e a qualsiasi altra tipologia di risorsa di proprietà dell'Ente.

Tutti i contratti che verranno conclusi tra l'Ente e terzi soggetti, ai quali viene permesso l'accesso ai dati, ai programmi informatici o ad mezzi altre strutture fisiche e non dell'Ente, dovranno riportare una clausola che impegni le parti a rispettare il presente documento; ciò indipendentemente dalla nomina a responsabile esterno del trattamento dati ai sensi del Regolamento UE 2016/679.

Nel caso di soggetto esterno, nominato responsabile del trattamento, questi deve impegnarsi a far rispettare il presente documento a tutti i propri dipendenti e ad eventuali altri soggetti.

Definizioni

Amministratori di Sistema: sono le figure, designate dal Titolare, che provvedono operativamente alla gestione e manutenzione del sistema informatico comunale sulla base delle misure organizzative fissate dal Responsabile del Servizio Informatico.

Custode delle Password: ove i sistemi informatici o le banche dati, non consentano una gestione automatizzata delle password (come avviene nell'Active Directory di Windows) e sia necessario tenere traccia di una password per iscritto, viene nominato un custode della password che provvede a conservarla. Possono essere nominati custodi diversi per password differenti, a seconda della necessità e del contesto organizzativo. Questa figura può coincidere con l'Amministratore di Sistema.

Dispositivo: qualsiasi strumento di elaborazione elettronica utilizzato per lo svolgimento delle attività che fanno capo all'organizzazione, il cui utilizzo rientra nel perimetro di competenza del presente disciplinare. Rientrano in tale definizione, a titolo esemplificativo e non esaustivo, desktop computer, notebook, tablet, ecc.

Ente: il Comune di Garbagnate Milanese.

GDPR: viene così definito nel presente documento il Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Incaricato Backup: è individuato dal Responsabile del Servizio Informatico e si occupa delle operazioni di backup dei dati sulla base delle istruzioni impartite dall'Amministratore di Sistema; per questa particolare mansione risponde direttamente all'Amministratore di Sistema; la sua designazione è effettuata per iscritto. Questa figura può coincidere con l'Amministratore di Sistema.

Incaricato (o Autorizzato) del Trattamento: è il soggetto persona fisica che effettua materialmente le operazioni di trattamento sui dati personali.

Responsabile del Servizio Informatico: è la figura designata che gestisce e coordina le attività di configurazione/aggiornamento dei sistemi e degli archivi informatici. Il ruolo del Responsabile del Servizio Informatico è solo quello di coordinatore dell'applicazione della normativa sulla riservatezza dei dati in ambito informatico, ferme restando le responsabilità dei singoli responsabili

in merito all'adozione degli atti (nomina incaricati, rilevazione banche dati, istruzione agli incaricati, ecc). Ai fini del presente regolamento, il Responsabile del Servizio Informatico è individuato nel Responsabile del Servizio Innovazione Tecnologica.

Responsabile del Trattamento dei dati: è la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare del trattamento (art. 4, par. 1, n. 8 GDPR).

Rilevazione: complesso di operazioni di analisi e verifica dei tracciamenti effettuati dai dispositivi svolte da amministratori di sistema a fronte di comprovate necessità definite nei capitoli seguenti del presente disciplinare.

Titolare del Trattamento dei dati (o anche solo Titolare): è "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le* **finalità** *e i* **mezzi** *del trattamento di dati personali*" (art. 4. par. 1, n. 7 GDPR).

Tracciamento: memorizzazione di eventi e operazioni effettuata automaticamente da un qualsivoglia dispositivo informatico, per finalità manutentive e di funzionamento dello stesso.

Funzionamento delle risorse informatiche

Le risorse informatiche tracciano una serie di eventi di sistema per attività amministrative, manutentive e di sicurezza, che variano a seconda della tipologia delle risorse stesse.
Il tracciamento di tali eventi non è oggetto di rilevazione da parte del servizio informatico. Qualora, per necessità manutentive o di gestione della sicurezza si rendesse necessario rilevare e/o registrare gli eventi tracciati di una risorsa specifica, tali trattamenti verranno preventivamente segnalati al personale aziendale coinvolto nelle modalità indicate nei successivi paragrafi.

Dati trattati attraverso le risorse informatiche concesse in dotazione

Le risorse informatiche sono messe a disposizione dall'Ente per finalità legate alle attività istituzionali dell'Ente stesso, pertanto l'utilizzo degli strumenti in dotazione deve essere di prevalente carattere professionale.
È consentito l'utilizzo per finalità personali della postazione di lavoro a condizione che lo stesso:

- venga effettuato al di fuori dell'orario di lavoro;
- non sia contrario alle regole di condotta indicate nei paragrafi successivi (oltre che del Regolamento di comportamento dei dipendenti) e non possa, in alcun modo, ledere l'immagine dell'Ente;
- non danneggi in alcun modo, diretto o indiretto, le proprietà dell'Ente;
- sia esplicito verso terzi che la responsabilità di qualsiasi operazione svolta per finalità personali sia imputabile esclusivamente all'utente.

È importante precisare che è consentito l'utilizzo personale, alle condizioni sopra specificate, esclusivamente delle risorse informatiche; non è in alcun modo consentito trattare dati di cui l'Ente è Titolare del Trattamento se non per attività di carattere professionale.
È ammessa la custodia di dati personali sulla postazione di lavoro a condizione che:

- siano riposti in cartelle di cui sia esplicitamente indicata la privatezza del dato (es. cartelle con dicitura "personale");
- vengano rimossi prima del rilascio della postazione di lavoro.

Alla riconsegna delle attrezzature da parte degli utenti all'Ente, questo potrà liberamente disporre di eventuali informazioni ivi presenti. Qualora le risorse informatiche riconsegnate dovessero

contenere dati personali relativi agli utilizzatori, il trattamento di tali dati verrà effettuato secondo i principi di pertinenza e non eccedenza previsti dalla normativa sulla protezione dei dati personali. Eventuali dati personali ancora residenti al momento della riconsegna della postazione verranno rimossi indiscriminatamente.
Tutti i dati e i documenti trattati durante lo svolgimento delle attività professionali, svolte in nome e per conto dell'Ente, sono di proprietà esclusiva dell'Ente stesso, pertanto devono essere lasciati a completa disposizione dell'Ente al momento della riconsegna delle attrezzature.

Utilizzo delle postazioni di lavoro

La postazione di lavoro affidata al dipendente è uno **strumento di lavoro**. Ogni utilizzo inadeguato può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

Non è consentito installare programmi provenienti dall'esterno salvo preventiva autorizzazione del Responsabile del Servizio Informatico, onde evitare il grave pericolo di introdurre minacce al sistema informatico nonché di alterare la stabilità delle applicazioni.

Non è consentito l'uso di software diversi da quelli messi a disposizione dall'Ente , in quanto l'inosservanza di questa disposizione, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'Ente a gravi responsabilità civili e penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (Legge 633 del 22 aprile 1941 sulla tutela della proprietà intellettuale, D.Lgs. 29 dicembre 1992 n. 518, sulla tutela giuridica del software e aggiornamenti successivi) che impone l'utilizzo di software regolarmente licenziati o opensource e quindi non preclusi dal diritto d'autore.

Il PC viene consegnato all'utente con una configurazione coerente con le misure organizzative e di sicurezza impostate dall'Ente stesso: non è consentito all'utente di modificare le caratteristiche impostate sul PC, salvo preventiva ed esplicita autorizzazione dell'Amministratore di Sistema.

Il PC deve essere spento prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio, salvo specifica disposizione dell'Amministratore di Sistema e/o a seguito di pianificazione dello spegnimento automatico. In ogni caso, poiché 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'uso indebito, l'utente che si allontana dalla postazione deve bloccarne l'uso tramite la combinazione dei tasti CTRL + ALT + CANC e successivo INVIO. È comunque previsto il blocco automatico delle postazioni di lavoro in caso di inattività per un certo periodo di tempo.

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna. Se il sistema non è impostato per scansionare automaticamente i dispositivi USB connessi, l'utente dovrà effettuare una scansione manuale con il software antivirus installato sulla postazione prima di accedere al contenuto del supporto removibile. Nel caso in cui vengano rilevati virus, l'utente deve avvertire immediatamente il Responsabile del Servizio Informatico e non deve per nessun motivo accedere al contenuto del supporto infetto. Non è consentito l'utilizzo di giochi o altre applicazioni di tipo ludico, anche se comprese nel sistema operativo installato.

Non sono permesse, a meno di specifiche e documentate autorizzazioni, le seguenti attività:

- caricare, memorizzare, pubblicare, diffondere, distribuire, tramite risorse dell'Ente documenti, informazioni, immagini, filmati ecc. in generale, ed in particolare:
    - a carattere violento, pornografico o contrario alla pubblica decenza, o suscettibile di mancare di rispetto agli esseri umani o alla loro dignità, con contenuto discriminatorio razziale ed etnico, contrario al buon costume, oltraggioso nei confronti dei minori, contrario all'ordine pubblico, diffamatorio o che contenga

contenuti illeciti penalmente o civilmente riconducibili a fattispecie qui non espressamente indicate;
    - pregiudizievoli per le risorse dell'Ente e per l'integrità e la conservazione dei dati dell'Ente stesso;
    - pregiudizievoli per l'immagine e il buon nome dell'Ente;
- accedere a server web (siti web) trattanti materie o soggetti ricadenti nelle categorie sopra elencate;
- tenere comportamenti che possano indurre taluno ad effettuare invii di materiale rientrante nelle tipologie sopra elencate; laddove l'utente si trovi a ricevere anche contro il suo volere tali materiali, è tenuto a informare il responsabile del Sistema Informativo e attenersi alle sue istruzioni circa il trattamento di tali materiali;
- utilizzare le risorse dell'Ente con fini di molestia, minaccia o comunque violando le norme di legge in vigore;
- caricare, memorizzare, trasmettere o utilizzare programmi, software, procedure od altra utilità che siano protetti dalle leggi sulla proprietà intellettuale, salvo che il Comune di Garbagnate Milanese ne detenga regolare licenza e/o autorizzazione del produttore;
- utilizzare strumentazioni, programmi, software, procedure, ecc. messi a disposizione dall'Ente in violazione delle leggi sulla proprietà intellettuale, delle regole di buona tecnica applicabili e delle prescrizioni emanate dall'Ente;
- caricare o trasmettere, con volontà, archivi o programmi contenenti virus o dati alterati;
- manomettere sistemi o archivi in maniera tale da inficiare la riservatezza, la disponibilità e l'integrità dei dati;
- inviare, con volontà, messaggi in massa ("spam") o favorire il propagarsi di notizie riconducibili a ciò che abitualmente viene definito "catena di S. Antonio";
- utilizzare le risorse dell'Ente in modo da consentire a soggetti non abilitati l'accesso ai dati e ad alle informazioni riservate, se non nei casi espressamente previsti dalla legge e dai regolamenti.

Poiché alcune attività sopra elencate possono avere conseguenze di natura penale, esse originano, in capo al trasgressore, tutte le responsabilità previste dalla legge.

Nonostante la presenza di programmi antivirus, è provato che l'utilizzo di applicazioni di comunicazione (internet, posta elettronica, ecc.) e di supporti di memoria rimovibili (CD, DVD, dispositivi USB ecc.) può comportare la trasmissione di malware o di programmi e archivi che alterano, distruggono e monitorano l'attività e i contenuti dei personal computer.

In caso di anomalie dell'hardware e del software affidatogli, l'utente deve immediatamente bloccarne l'operatività, fermare le eventuali elaborazioni in corso (bloccare l'elaborazione dalla gestione attività e scollegare il cavo di rete) ed informare immediatamente l'Amministratore di Sistema.

Utilizzo dei supporti mobili e PC portatili

Tutti i supporti riutilizzabili (secure drive, CD, DVD, chiavi e dischi esterni USB, ecc…) contenenti dati particolari (c.d. "sensibili") e giudiziari devono essere gestiti con particolare cautela onde evitare che il loro contenuto possa essere trattato da soggetti non incaricati.

I supporti fissi e rimovibili, contenenti dati particolari (sensibili) e/o giudiziari, non possono essere portati all'esterno della sede comunale, all'interno della quale devono comunque essere custoditi in archivi chiusi a chiave.

Ove sia necessario portare dati particolari (sensibili) e/o giudiziari all'esterno degli edifici comunali si dovranno concordare le modalità con il servizio informatico, che provvederà a valutare le necessità e a dare le opportune istruzioni sul mezzo e sulla modalità più idonei (ad es. memoria USB protetta da pincode, da password o da dati biometrici).

L'utente è responsabile delle attrezzature informatiche portatili assegnategli dal servizio informatico e deve custodirle con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai portatili si applicano le regole di utilizzo previste per i PC connessi alla rete, con particolare attenzione alla rimozione di eventuali file elaborati sugli stessi prima della riconsegna.

Gli utenti di PC portatili si impegnano, dovunque dovessero trovarsi, a mettere in sicurezza gli strumenti in dotazione e i dati ivi contenuti.

Danni arrecati alle attrezzature ed ai PC o la loro perdita dovuti ad incauta custodia saranno a carico dell'utente utilizzatore.

Non è consentito l'utilizzo sul PC di dispositivi di memorizzazione non preventivamente autorizzati dal Responsabile del Servizio Informatico. È consentito collegare e/o connettere il dispositivo mobile a reti e altri apparati di proprietà dell'utilizzatore durante il lavoro in modalità agile: in tal caso, l'utilizzatore si assume la responsabilità sulla sicurezza degli apparati e della rete a cui il PC dovesse essere connesso. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna e alle connessioni esterne alla rete dell'Ente. Prima dell'apertura del supporto deve provvedere alla sua scansione tramite il software antivirus. L'utente deve avvertire immediatamente il Responsabile del Servizio Informatico nel caso in cui vengano rilevati virus sul supporto e/o nel caso in cui dovesse emergere una infezione/infiltrazione – anche solo potenziale – conseguente all'utilizzo di un supporto esterno o di una rete non adeguatamente controllata.

Accesso remoto alle risorse informatiche dell'Ente

Nel caso in cui sia necessario consentire ad un utente l'accesso remoto alle risorse informatiche dell'Ente, questo deve essere preventivamente concordato con il Responsabile del Servizio Informatico; in ogni caso, l'utente dovrà attenersi scrupolosamente alle istruzioni impartite e ad eventuali disposizioni regolamentari adottate dall'Ente.

Utilizzo della rete LAN e delle risorse condivise

Al fine di garantire la disponibilità dei dati e un'efficace politica di backup, gli utenti devono salvare su cartelle di rete tutti i file di lavoro ed astenersi dal salvarli sul disco locale della postazione di lavoro (si specifica che la cartella "desktop" si trova sulla postazione in locale, pertanto è inadatta al salvataggio dei file perché non sottoposta a procedure di backup).

Le cartelle/unità di rete 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 può essere dislocato, nemmeno per brevi periodi, in queste unità.

Sulle cartelle/unità di rete vengono svolte regolari attività di amministrazione e backup.

Le credenziali di accesso alla rete ed ai programmi sono personali e nominative; è assolutamente vietato accedere alla rete e ai programmi con credenziali altrui. Sono tollerate, sino a completo adeguamento dei software, le credenziali identificative di un servizio/ente (non differenziabili per utente) fornite per alcuni gestionali.

Le cartelle su server sono organizzate nella maniera seguente:

- una cartella per ogni settore/servizio condivisa in maniera esclusiva dai soggetti che vi operano;
- una cartella condivisa da tutti gli uffici per consentire l'interscambio di documenti.

Per la trasmissione di file all'interno dell'Ente è possibile utilizzare la posta elettronica con l'apposita funzione Drive opportunamente condivisa, oppure è possibile utilizzare le cartelle di scambio create a tale scopo. Le cartelle di scambio devono essere tenute in ordine, eliminando i file non più necessari anche al fine di non consentire il trattamento dei dati a persone non espressamente incaricate; non devono assolutamente essere utilizzate per scambio di file contenenti dati particolari (c.d. "sensibili") o giudiziari.

Gli del autorizzati al trattamento dovranno coordinare la periodica pulizia degli archivi (almeno ogni 6 mesi) attuando:

- la cancellazione dei file obsoleti ed inutili nelle cartelle di competenza;
- l'eliminazione delle archiviazioni ridondanti, che dovranno comunque essere evitate;
- la verifica delle cartelle in coerenza con il trattamento dei dati da parte degli uffici e dei gruppi di lavoro;
- la verifica ed eventualmente la variazione, avvalendosi dell'Amministratore di Sistema, delle "permission" di accesso a risorse condivise affinché siano coerenti con le del autorizzazione al trattamento dati e le disposizioni sulla fascicolazione.

L'Amministratore di Sistema, nell'espletamento delle mansioni attribuitegli dal Responsabile del Servizio Informatico, può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà pericolosi per la sicurezza, sia sui PC collegati alla rete sia sui server. Potrà inoltre ricorrere alla cancellazione di alcune tipologie di file al fine di liberare spazio disco sui server: tale operazione, di carattere manutentivo, verrà comunicata preventivamente agli utenti, che potranno segnalare eventuali eccezioni all'operazione di pulizia a fronte di motivazioni di carattere esclusivamente lavorativo.

Il collegamento alla rete comunale di pc portatili o di attrezzature informatiche non di proprietà del Comune di Garbagnate M.se è vietato.

Il Responsabile del Servizio Informatico potrà consentire deroghe a quanto previsto dal precedente paragrafo solo in casi eccezionali, dopo attenta valutazione, e dietro adeguata supervisione da parte di personale incaricato dal Servizio Innovazione Tecnologica dell'Ente.

Per quanto riguarda l'utilizzo di stampanti condivise, gli utenti dovranno effettuare la stampa dei dati solo se strettamente necessaria e dovranno ritirarla prontamente dai vassoi delle stampanti comuni.

Acquisizione software

Sulle postazioni è consentita l'installazione esclusiva delle seguenti categorie di software:

- software commerciale dotato di licenza d'uso
- software gestionale realizzato specificatamente per l'Amministrazione comunale dalle ditte specializzate nel settore della P.A.
- software realizzato specificatamente dagli organi centrali della Pubblica Amministrazione o Enti nazionali

- software gratuito e shareware prelevato dai siti internet, solo se espressamente autorizzato dal Responsabile del Servizio Informatico.
- qualsiasi altro software si renda necessario per l'esercizio delle attività lavorative e istituzionali, previa autorizzazione del Responsabile del Servizio Informatico da richiedersi per iscritto a mezzo mail.

L'acquisto e la conseguente installazione di software devono essere sempre preventivamente valutati, autorizzati ed effettuati in collaborazione con il Responsabile del Servizio Informatico, al fine di garantire la sicurezza e la stabilità dei sistemi e la compatibilità del software con gli stessi.

Servizi con impatto sui sistemi informatici

L'acquisizione di materiale hardware o di qualsiasi dispositivo che interagisca con la rete e/o la strumentazione informatica comunale o che possa avere un impatto su di essi, qualora non venga eseguita direttamente dal Responsabile del Servizio Informatico, deve essere concordata preventivamente con questo, onde evitare problematiche di funzionamento, cadute prestazionali o altri problemi alla sicurezza e all'immagine dell'Ente.

Qualora nell'esercizio di una funzione amministrativa sia prevista la fornitura di software accessorio alla gestione/erogazione di un servizio, l'ufficio competente provvede a consultare il Responsabile del Servizio Informatico nelle **fasi preliminari** del processo di acquisizione, per la corretta definizione delle caratteristiche del software, affinché lo stesso risulti:

- compatibile con il sistema informativo comunale,
- conforme alle misure di sicurezza adottate dall'Ente con particolare riguardo alla sicurezza degli accessi
- certificato per l'installazione sulle macchine in dotazione all'Ente (server e pc)
- installato correttamente

In caso di mancata consultazione preventiva del Responsabile del Servizio Informatico non potrà essere effettuata alcuna installazione.

Qualora venga affidata all'esterno la gestione di dati comunali per l'erogazione di servizi, l'ufficio competente **deve concordare preventivamente** con il Responsabile del Servizio Informatico le modalità e i formati con cui tali dati devono essere scambiati sia in ingresso che in uscita e le condizioni di restituzione dei dati al termine del rapporto di collaborazione.

Gestione delle password e degli accessi

L'utente deve utilizzare sempre una password quando viene richiesto dalla procedura, avendo cura che nessuno ne venga a conoscenza.

Le credenziali di accesso al dominio e dello screensaver sono previste e vengono attribuite dall'Amministratore di Sistema all'utente per il primo accesso. Dopo il primo accesso il sistema chiederà all'utente di modificare la password, stesso che dovrà rimanere segreta. Qualora si rendesse necessario (per manutenzione, aggiornamenti, assenza prolungata imprevista che renda indisponibili risorse gestite dall'utente, altre situazioni d'urgenza) l'accesso dell'Amministratore al sistema con le credenziali dell'utente, si procederà previa modificata della password di accesso.. Al successivo accesso da parte dell'utente, l'Amministratore rilascerà una password temporanea che verrà immediatamente modificata dall'utente.

L’accesso agli applicativi può a sua volta essere regolato da un’ulteriore password: le modalità di gestione e di scadenza della password sono specifiche per ogni accesso. All’utente sarà fornito un profilo personale e verranno attivate procedure per garantirgli la conoscenza esclusiva della password. Nel caso il sistema non lo consenta o sia necessario l’intervento dell’Amministratore di Sistema per garantire la disponibilità dei dati, verranno concordate procedure specifiche per la gestione degli accessi fra il Responsabile del Sistema Informatico e il responsabile del servizio.

La combinazione dell’accesso al dominio e agli applicativi è necessaria per garantire il rispetto di standard minimi di sicurezza nonché l’adeguatezza delle misure previste per il rispetto della normativa relativa alla protezione dei dati personali.

Le password del dominio e degli applicativi, salvo impossibilità dovute all’obsolescenza del software, devono essere modificate ogni 3 mesi, devono essere formate da almeno una lettera minuscola, una maiuscola, un numero e un carattere speciale; devono essere composte da almeno otto caratteri e non devono contenere riferimenti agevolmente riconducibili all’incaricato.

Nel caso in cui si sospetti che una password abbia perso la segretezza, l’utente provvederà, ove possibile, a modificarla personalmente, altrimenti provvederà a modificarla con il supporto del Servizio Innovazione Tecnologica.

Non è consentito utilizzare il profilo personale di altri soggetti per connettersi al dominio o agli applicativi. Qualora l’utente venisse a conoscenza delle password di un altro utente, è tenuto a darne immediata notizia all’Amministratore di Sistema.

Le password non devono essere riutilizzate. Nel caso di inserimento di password errata, dopo il quinto tentativo, il profilo dell’utente verrà disabilitato e ne deve essere data comunicazione all’Amministratore di sistema.

È fatto assoluto divieto di esporre o di rendere facilmente accessibile documentazione riportante le password di accesso (ad esempio bigliettini sui monitor, fogli delle password, annotazioni su fogli, quaderni o documenti informatici) o di condividere le password tramite email o canali di messaggistica.

Attività di backup

Sono oggetto di attività di salvataggio centralizzato anche su supporti esterni:

- i file salvati sulle cartelle/unità di rete messe a disposizione dal servizio informatico;
- le macchine virtuali installate sugli host.

Gli elementi sopra indicati vengono salvati sistematicamente di notte (una volta al giorno). Viene effettuato inoltre un backup settimanale su 3 dischi alternati (ciascuno con capienza di 2 backup completi), per una conservazione complessiva di 6 backup settimanali consecutivi, oltre ad un ulteriore backup mensile.

Un backup annuale viene conservato in luogo sicuro in edificio separato dai plessi comunali.

I dati che risiedono sulle postazioni PC (in locale) non sono soggetti a operazioni di backup centralizzato.

Per quanto riguarda eventuali archivi localizzati sulle postazioni di lavoro, gli utenti devono concordare, sotto loro responsabilità, l’attività di backup insieme al Servizio Innovazione Tecnologica.

Attività e strumenti di assistenza remota

Per finalità di carattere manutentivo sono attivi, presso l'Ente, strumenti di assistenza remota che consentono, agli operatori incaricati dal Responsabile del Servizio Informatico, di connettersi alle postazioni degli utenti per fornire supporto in tempo reale ed assistere gli utenti nella risoluzione di problematiche di carattere informatico.

Gli strumenti utilizzati manifestano esplicitamente la connessione alla postazione da parte dell'operatore: l'utente dovrà consentire tramite autorizzazione verbale o informatica l'intervento remoto.

Per quanto riguarda gli interventi di assistenza remota sulle postazioni da parte di Amministratori esterni, detti interventi dovranno comunque essere preventivamente concordati con il Responsabile del Servizio Informatico e comunque comunicati al servizio stesso.

Posta elettronica

La casella di posta elettronica, assegnata dall'Ente all'utente, è uno strumento di lavoro.

Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

Qualsiasi attività istituzionale realizzata tramite utilizzo di posta elettronica deve essere svolta con l'esclusivo utilizzo di caselle registrate sotto il dominio di posta istituzionale dell'Ente o tramite caselle di posta elettronica certificata registrate dall'Ente stesso.

È fatto divieto di utilizzare le caselle di posta elettronica comunale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list salvo diversa ed esplicita autorizzazione da parte del Responsabile del Servizio Informatico per esigenze di lavoro.

È inoltre da evitare, ove possibile, l'invio di messaggi con allegati di grandi dimensioni, al fine di evitare eventuali sovraccarichi al sistema informativo e nuocere all'efficacia della comunicazione.

La casella di posta deve essere tenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

Per la trasmissione di file all'interno dell'Ente è possibile utilizzare la posta elettronica, con l'apposita funzione Drive opportunamente condivisa,, oppure è possibile utilizzare le cartelle di scambio create a tale scopo.

È vietato inviare mail con allegati contenenti file eseguibili (estensione .exe, .bat, ecc.).

È vietato inviare catene telematiche (o di S. Antonio). Se si dovessero ricevere messaggi di tale tipologia, si dovrà provvedere alla cancellazione del messaggio ricevuto senza divulgarlo in alcun modo. Non si dovranno in alcun caso attivare gli allegati di tali messaggi.

Qualora si ricevessero messaggi sospetti di richiesta di password o altre informazioni oppure di invito a svolgere operazioni sulla propria postazione di lavoro (es. apertura o cancellazione di file, installazione aggiornamenti, ecc), l'utente è tenuto a segnalarli immediatamente all'Amministratore di Sistema prima di effettuare qualsiasi azione.

Al fine di garantire la continuità di servizio, sono previste 2 differenti modalità per la gestione delle assenze, programmate o non, degli operatori preposti alla lettura dei messaggi di una specifica casella di posta:

1) ASSENZA PROGRAMMATA: attivazione da parte dell'utente di un risponditore automatico che segnali la temporanea indisponibilità all'accesso alla casella di posta, indicando eventualmente una casella di posta alternativa a cui inviare il messaggio;
2) ASSENZA NON PROGRAMMATA: in caso di assenza non programmata, è opportuno che l'utente, se possibile, si colleghi al sistema di posta elettronica per attivare il risponditore automatico, come indicato al punto precedente. In caso di impossibilità, da parte dell'utente assente, il responsabile del Servizio, se ritiene opportuno, può richiedere al Servizio Informatico l'impostazione del risponditore automatico o il recupero di specifiche mail formalizzando specifica richiesta scritta al Responsabile del Servizio Innovazione Tecnologica.

È vietato utilizzare client di posta elettronica; le caselle mail devono essere utilizzate esclusivamente via web. Le caselle di posta elettronica in uso presso l'Ente sono di 2 tipologie:

1) caselle nominative, assegnate con lo standard *<nome>.<cognome>*@comune.garbagnate-milanese.mi.it Tali caselle sono intestate personalmente agli utenti: è importante sottolineare che, nonostante le caselle siano intestate ad un individuo, sono da considerarsi uno strumento aziendale e non corrispondenza privata; pertanto, l'utilizzo verso destinatari esterni dovrà essere consono con le funzioni istituzionali svolte dall'Ente. La divulgazione dell'indirizzo personale deve essere limitata ai soli casi in cui non possa essere divulgato l'indirizzo di posta relativo all'ufficio di appartenenza.
2) Caselle di posta assegnate ad un ufficio o ad una funzione sul dominio *<nomeufficio>*@comune.garbagnate-milanese.mi.it. Tali caselle possono essere assegnate ad una o più persone che hanno in solido la responsabilità di garantire continuità nella gestione della corrispondenza. In caso siano assegnate ad una sola persona, questa ha la responsabilità di garantire la continuità nella gestione della corrispondenza; in caso di sua indisponibilità, programmata o non, verrà attivata una delle 2 differenti modalità per la gestione delle assenze indicate precedentemente.

   L'Amministratore di Sistema, nell'espletamento delle sue funzioni, potrà accedere alle caselle di posta assegnate per finalità manutentive solo in presenza dell'assegnatario (o su sua esplicita autorizzazione) della casella o su richiesta del diretto superiore in caso di indisponibilità dell'assegnatario.

In ogni caso l'Ente si impegna a rispettare la confidenzialità dei messaggi elettronici di provenienza o a destinazione di recapiti sindacali (contenuto, autori e destinatari), delle mailing list elaborate e scambiate in rete da organismi sindacali, ecc.

Internet

Il collegamento ad Internet è uno strumento messo a disposizione per finalità di carattere lavorativo: è consentita la navigazione in internet per motivi diversi da quelli strettamente legati all'attività lavorativa a condizione che:

- venga effettuata al di fuori dell'orario di lavoro;
- non sia contraria alle regole di condotta indicate nel presente disciplinare e non possa in alcun modo ledere l'immagine dell'Ente;
- non danneggi in alcun modo, diretto o indiretto, le proprietà dell'Ente;
- sia esplicito verso terzi che la responsabilità di qualsiasi operazione svolta per finalità personali sia imputabile esclusivamente all'utente.

Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza per cui va assolutamente evitato l'utilizzo inappropriato dello stesso.

Pertanto, per garantire quanto previsto dalla Legge e secondo le direttive emanate dal Garante per la protezione dei dati personali, al fine di evitare abusi ed evitare il monitoraggio del traffico telematico, è attivo un filtro che blocca l'accesso ai siti ritenuti palesemente non pertinenti con le attività istituzionali. Il filtro adottato utilizza sistemi euristici di scarto di siti facenti parte di categorie appositamente selezionate. Qualora, per lo svolgimento della attività istituzionali, un utente necessitasse di accedere a un sito scartato dai sistemi di filtraggio, potrà richiederne l'accesso al Responsabile del Servizio Informatico, per tramite del responsabile del servizio che se ne assume la responsabilità.

È fatto assoluto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato dai siti internet, se non espressamente autorizzato dall'Amministratore di Sistema.

A fini statistici, di qualità del servizio e di sicurezza, l'occupazione di banda generata dal traffico internet e dallo scambio di posta elettronica potrà essere soggetta a controlli da parte dell'Ente sotto forma di dati aggregati ed anonimi, in osservanza dei limiti posti dalla legge in materia di riservatezza.

Qualora i sistemi di sicurezza segnalino delle potenziali criticità che possano minare l'integrità dei dati e la stabilità del sistema stesso, potrebbero essere effettuati dei controlli sulla navigazione internet. Tali controlli saranno preventivamente segnalati al personale e si opereranno secondo stadi successivi:

1) controlli generici sulle pagine visitate, senza che vengano tracciati gli utenti che le visitano;
2) controlli aggregati sulle pagine visitate con suddivisione del traffico effettuato per aree;
3) controlli specifici sulle pagine visitate, con tracciamento dell'indirizzo IP da cui si effettua la visita o dell'utente che la effettua.

Il tracciamento specifico verrà effettuato solo qualora il trattamento generico e quello aggregato non abbiano consentito di risolvere le criticità riscontrate e verrà comunque nuovamente segnalato in forma preventiva agli utenti.

Tutti i dati di traffico internet potranno comunque essere sottoposti a tracciamento da parte di sistemi automatici implementati presso l'Ente e custoditi per limitati periodi di tempo. La consultazione di tali dati, al di fuori dei casi indicati precedentemente, è consentita solo alle forze dell'ordine per attività di carattere ispettivo consentite dalla normativa sulla privacy.

Intranet

L'Ente mette a disposizione del personale una apposita area di condivisione della conoscenza accessibile all'interno della rete locale dell'Ente, contenente guide, corsi, FAQ, regolamenti, normative, best practice, policy, materiale informativo, modelli documentali, etc.

Tale base di conoscenza è accessibile da qualsiasi dispositivo collegato alla rete dell'Ente, anche nel caso di connessione dall'esterno attraverso VPN.

La Intranet sarà mantenuta aggiornata dal Responsabile del Servizio Informatico e dai suoi collaboratori; contestualmente all'aggiornamento, saranno pubblicati periodici comunicati sia nella pagina principale della Intranet che nel canale Telegram predisposto per il personale.

Ogni dipendente dell'Ente dovrà prendere visione delle comunicazioni pubblicate sulla Intranet.

In caso di necessità di informazioni, ogni dipendente dovrà primariamente verificare la presenza di materiale all'interno della Intranet; solo in caso di assenza potrà rivolgere richieste e/o istanze al Responsabile del Servizio Informatico o ad altro personale di ruolo presso il Servizio Innovazione Tecnologica.

Il servizio Intranet è ad uso esclusivo dell'Amministrazione del Comune di Garbagnate Milanese. E' fatto assoluto divieto di rendere accessibile la Intranet a terzi e/o di comunicare il contenuto della stessa – anche parzialmente – al di fuori del perimetro di sicurezza dell'Ente. La consultazione della Intranet comunale è obbligatoria e l'utente è tenuto ad effettuarla con frequenza durante la giornata lavorativa.

Social Networks

Non è consentito l'utilizzo di social networks durante l'orario di lavoro, a meno che tali piattaforme non vengano espressamente impiegate in maniera strumentale per lo svolgimento delle proprie attività lavorative.

È assolutamente vietato esprimere opinioni su informazioni acquisite durante lo svolgimento delle proprie attività istituzionali e condividere informazioni e riferimenti di carattere professionale che in qualche modo possano ledere l'immagine dell'Ente. Tale divieto è da intendersi anche al di fuori dell'orario di lavoro ed eventualmente oltre la cessazione della collaborazione professionale con il Comune.

Per qualsiasi danno, che potesse derivare all'immagine dell'Ente, imputabile a comportamenti non conformi alle indicazioni sopra riportate e comunque contrari alle norme sulla pubblica amministrazione, il Comune potrà applicare al trasgressore un provvedimento disciplinare ed eventuali sanzioni previste dalla legge.

Sicurezza generale e perimetrale

Presso l'Ente è attivato un sistema di sicurezza perimetrale a difesa dei sistemi e dei dati comunali, che traccia eventi che possono essere indizio di minacce informatiche. Il sistema è soggetto a procedure di aggiornamento automatico per quanto riguarda la lista e le caratteristiche delle minacce.

Il perimetro è gestito dal Responsabile del Servizio Informatico, anche per il tramite di propri incaricati, il quale effettua attività di verifica delle segnalazioni attivate dal sistema stesso, con lo scopo di comprendere e prevenire eventuali minacce esterne.

Qualora il sistema attivato rilevi delle minacce a specifici indirizzi IP interni, il Responsabile del Servizio Informatico verificherà le cause del pericolo rilevato insieme all'utente/utenti che abitualmente utilizza/utilizzano la postazione, con l'obiettivo di comprendere la natura dell'intrusione e prevenire eventuali danni.

Una volta individuate le cause dell'evento verranno adottati provvedimenti correttivi, con segnalazione al Titolare del Trattamento di eventuali violazioni alle regole indicate nel presente disciplinare.

Telefonia mobile e dispositivi che consentono la navigazione internet

Tutti i dispositivi di telefonia mobile e che consentono la navigazione internet attraverso un piano tariffario a carico dell'Ente, costituiscono uno strumento di lavoro e attività istituzionale, pertanto gli eventuali affidatari devono prestare adeguate cautele durante il loro utilizzo.

I dati contabili relativi al traffico telefonico ed internet potranno essere analizzati dall'Ente al fine di consentire un adeguato controllo e contenimento dei costi. I numeri telefonici presenti nei dati di traffico saranno oscurati nelle ultime tre cifre, per cui non sarà possibile risalire ai numeri contattati.

È fatto obbligo proteggere l'accesso al dispositivo in dotazione attraverso l'importazione di PIN, segno, password e/o dati biometrici.

L'utilizzatore dovrà attenersi alle istruzioni impartite dal Responsabile del Servizio Informatico, installando ed aggiornando ogni applicativo indicato e/o richiesto. In particolare, i dispositivi di telefonia mobile con funzioni avanzate (c.d. "smartphone") dovranno essere dotati di specifico software client per la gestione della posta elettronica nonché di software di messaggistica adottati dall'Ente.

Se lo smartphone non dovesse essere fornito completamente configurato, l'utilizzatore è tenuto a configurare la propria utenza e la propria posta elettronica; successivamente dovrà installare l'app di messaggistica "Telegram" e iscriversi all'apposito canale del Comune di Garbagnate M.se creato per il personale dipendente.

Il servizio CED provvede ad installare il servizio di messaggistica Telegram su tutti i telefoni di servizio. Il personale ha obbligo di consultare quotidianamente il canale Telegram dedicato In caso di attivazione di modalità di lavoro agile al di fuori delle strutture comunali, è fatto obbligo per l'utente, fornito di smartphone e/o SIM di provvedere alla deviazione delle chiamate del proprio interno d'ufficio verso la numerazione mobile assegnatagli.

Danni arrecati ai dispositivi, agli accessori in dotazione o la loro perdita, dovuti ad incauta custodia, saranno a carico dell'utente utilizzatore.

A causa della sempre maggiore interazione tra i dispositivi telefonici e informatici, l'abuso di tali strumenti può costituire una potenziale fonte di minaccia ai sistemi dell'Ente. Pertanto è vietato:

- installare applicazioni sui dispositivi cellulari senza prima aver concordato la modalità o possibilità con il Responsabile del Servizio Informatico;

- installare sulle postazioni di lavoro in ufficio programmi di sincronizzazione/backup dei dati contenuti sui dispositivi cellulari senza la preventiva autorizzazione del Responsabile del Servizio Informatico;

- apportare interventi sulle configurazioni del dispositivo o sulle condizioni di servizio che possano incidere in maniera rilevante sui consumi senza averlo concordato con il Responsabile del Servizio Informatico.

Al momento della restituzione dei dispositivi, il personale assegnatario dovrà cancellare i dati contenuti sul cellulare (es. Rubrica telefonica, SMS, contenuti multimediali, ecc). Qualora il dispositivo restituito contenga dati personali, questi verranno cancellati senza alcuna verifica preventiva.

Per quanto riguarda gli aspetti concernenti i consumi telefonici e il traffico internet, generati dai dispositivi gli stessi vengono comunicati verbalmente in fase di assegnazione del bene ed aggiornati, a stesso mezzo, in caso di modifiche al piano tariffario.

Videosorveglianza

Al fine di tutelare la proprietà dell'Ente sono presenti, all'esterno di alcune sedi comunali, sistemi di videosorveglianza.

La collocazione delle telecamere e gli estremi identificativi delle persone fisiche incaricate del trattamento dei dati, con l'elenco delle funzioni ad essi attribuite, vengono rese note all'interno dell'organizzazione da parte del Responsabile del Settore di Polizia Locale in accordo con il Titolare del Trattamento.

L'Ente assicura in ogni caso il rispetto della normativa in materia di tutela dei lavoratori.

Attività dell'Amministratore di Sistema

S'intende per Amministratore di Sistema qualsiasi soggetto le cui funzioni di gestione ed amministrazione di sistemi informatizzati rendano ad esso tecnicamente possibile l'accesso, anche fortuito, a dati personali. In questa definizione rientrano pertanto le funzioni tecnicamente definite di amministratore di sistema (*system administrator*), amministratore di base di dati (*database administrator*) e amministratore di rete (*network administrator*).

L'Amministratore di Sistema è designato dal Titolare in forma scritta o designato tramite apposito contratto di servizio stipulato con un Responsabile del Trattamento in outsourcing. La designazione quale Amministratore di sistema deve essere conforme alle normative sulla protezione dei dati personali e ai provvedimenti relativi emanati dal Garante della Privacy sull'argomento.

Deve inoltre recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

Fra le funzioni dell'Amministratore di sistema, sia esso interno all'Ente che esterno, vi possono essere:

- sovrintendere al funzionamento della rete, comprese le apparecchiature di protezione (firewall, filtri);
- monitorare lo stato dei sistemi, con particolare attenzione alla sicurezza;
- effettuare e/o coordinare interventi di manutenzione hardware per i dispositivi di competenza;
- effettuare interventi di manutenzione software su sistemi operativi e applicativi di competenza;
- coordinare e sovrintendere l'operato di eventuali tecnici esterni all'Ente (nel caso di Amministratore interno);
- coordinare a livello operativo la gestione e la distribuzione dei profili di accesso e delle password degli utenti del sistema e/o dei sottosistemi di competenza nel rispetto delle normative relative alla protezione dei dati personali;
- gestire le password di amministrazione di sistema o dei sottosistemi di competenza;
- collaborare con i responsabili del trattamento dei dati personali per l'organizzazione delle politiche di sicurezza;
- informare il responsabile dei sistemi informatici e/o il titolare sulle non corrispondenze con le norme di sicurezza e su eventi di sicurezza rilevanti.

Osservanza delle regole sulla privacy

Oltre a quanto indicato nel presente documento, è obbligatorio attenersi alle disposizioni in materia di privacy e di misure di sicurezza ai sensi del Regolamento UE nr. 2016/679.

Osservanza del presente disciplinare

La finalità del presente documento è quella di regolamentare l'utilizzo delle risorse informatiche aziendali, al fine di garantire l'adeguata riservatezza, integrità e disponibilità dei dati gestiti dall'Ente.

A tali scopi, in caso si riscontrassero delle criticità che possano ledere la sicurezza del sistema informativo, l'Ente potrà verificare che l'utilizzo delle risorse informatiche concesse in dotazione agli utenti sia conforme alle indicazioni riportate nel presente disciplinare. Qualora l'utilizzo delle risorse informatiche possa in qualche maniera rivelare dati personali relativi agli utilizzatori, la rilevazione verrà effettuata secondo i principi di pertinenza e non eccedenza del trattamento dei dati rispetto alle finalità di sicurezza per cui tali dati sono trattati.

Il mancato rispetto delle regole e delle misure di sicurezza elencate nel presente documento implica la responsabilità personale dell'utente.

I fatti negativi e/o pregiudizievoli espongono il trasgressore oltre che all'apertura di specifico procedimento disciplinare, alle sanzioni previste dalla legge e al risarcimento degli eventuali danni causati.

Entrata in vigore

Il presente documento è in vigore a partire dalla data di esecutività del provvedimento che lo approva.

Gli uffici competenti provvederanno a consegnare al momento dell'assunzione ad ogni utente copia digitale del presente disciplinare.