



COMUNE DI CAIVANO

CITTA' METROPOLITANA DI NAPOLI
Servizio Informatizzazione

Regolamento sull'utilizzo e la gestione delle risorse informatiche comunali.



COMUNE DI CAIVANO

CITTA' METROPOLITANA DI NAPOLI
Servizio Informatizzazione

Sommario

Introduzione	3
1. Indicazioni generali	5
1.1. Finalità della Policy	5
1.2. Campo di applicazione.....	5
1.3. Destinatari.....	5
1.4. Entrata in vigore del regolamento e diffusione	5
1.5. Verifiche	6
1.6. Sanzioni.....	6
2. Politiche ed utilizzo delle risorse informatiche comunali	7
2.1 Indicazioni generali	7
2.2 Configurazioni dei dispositivi comunali e collegamento alla rete comunale	8
2.3 Installazione di hardware e software	8
2.4 Supporti di memorizzazione	8
2.5 Stampa su stampanti di rete	9
2.6 Scansione da stampante multifunzione con salvataggio su cartella di rete:	9
2.7 Credenziali per l'accesso ai dispositivi e alla rete comunale	9
2.8 Caratteristiche delle credenziali di accesso.....	10
2.9 Unità di rete e cartelle condivise	11
2.10 Diritti di accesso e controllo remoto	12
3. Utilizzo della rete Internet e dei relativi servizi	13
3.1. Regole di utilizzo di internet nelle sedi comunali	13
4. Posta elettronica	15
4.1. Casella di posta elettronica comunale	15
4.2. Credenziali per l'accesso alla casella di posta elettronica	15
4.3. Utilizzi consentiti della posta elettronica	16
4.4. Contenuto dei messaggi	18
4.5. Altre istruzioni riguardanti la posta elettronica	19
Terminologie e abbreviazioni	20



COMUNE DI CAIVANO

CITTA' METROPOLITANA DI NAPOLI
Servizio Informatizzazione

Introduzione

Il presente Regolamento intende fornire ai dipendenti e collaboratori del Comune di Caivano (di seguito più semplicemente indicati come "Utenti"), le indicazioni per una corretta ed adeguata gestione delle informazioni personali, in particolare attraverso l'uso di sistemi, software e strumenti informatici dell'Ente.

Si specifica che tutto ciò che sono utilizzati dagli Utenti, intendendo con ciò le postazioni di lavoro (PDL, ovvero PC, notebook, tablet, smartphone,...), risorse fisiche (es: server, NAS, dischi esterni o chiavette USB, armadi dati o locali adibiti a datacenter) o logiche (es: aree di lavoro condivise), caselle di posta elettronica (e-mail istituzionali o personali) ed altri strumenti con relativi software e applicativi (di seguito più semplicemente indicati come "Strumenti"), **sono messi a disposizione dall'Ente** per rendere la prestazione lavorativa.

Gli Strumenti, nonché le relative reti di trasmissione dati dell'Ente a cui è possibile accedere tramite gli stessi, **sono domicilio informatico del Comune di Caivano**.

I dati personali e le altre informazioni dell'Utente che sono registrati negli Strumenti o che si possono eventualmente raccogliere tramite il loro uso, **sono utilizzati per finalità istituzionali, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente**.

Per tutela del patrimonio dell'Ente si intende altresì **la sicurezza informatica e la tutela del sistema informatico dell'Ente**.

Tali dati personali ed informazioni sono altresì utilizzabili **a tutti e solo ai fini connessi al rapporto di lavoro**, visto che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli Strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Regolamento Europeo 679/16 sulla protezione dei dati personali.

Viene, infine, precisato che non sono installati o configurati sui sistemi informatici in uso agli utenti apparati hardware o strumenti software aventi come scopo il controllo a distanza dell'attività dei lavoratori, ma solo per il monitoraggio del sistema informativo ai fini di garantirne la sicurezza (es: antivirus).

Eventuali attività di assistenza remota sui strumenti informatici in uso agli utenti vengono effettuate solo dopo l'assenso da parte degli stessi.

Il presente Regolamento è redatto:

- alla luce della Legge 20.5.1970, n. 300, recante "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento";
- in attuazione del Regolamento Europeo 679/16 sulla protezione dei dati personali (d'ora in avanti Reg. 679/16 o GDPR);
- in attuazione del D. Lgs. n. 196 del 2003, modificato dal D.Lgs. n. 101 del 2018 (d'ora in avanti Codice Privacy);
- ai sensi delle "Linee guida del Garante per posta elettronica e internet" in Gazzetta Ufficiale n. 58 del 10 marzo 2007;



COMUNE DI CAIVANO

CITTA' METROPOLITANA DI NAPOLI
Servizio Informatizzazione

- nel rispetto delle funzioni ed indirizzi del “Responsabile per la transizione al digitale” (RTD) così come definite dall’art.17 del Codice dell’Amministrazione Digitale (D.Lgs.82/2005 e ss.mm.ii., d’ora in avanti CAD);
- in attuazione della circolare AGID 2/2017 “Misure minime di sicurezza ICT per le pubbliche amministrazioni”;
- alla luce dell’articolo 23 del D.Lgs. n. 151/2015 (c.d. Jobs Act) che modifica e rimodula la fattispecie integrante il divieto dei controlli a distanza, nella consapevolezza di dover tener conto, nell’attuale contesto produttivo, oltre agli impianti audiovisivi, anche degli altri strumenti «dai quali derivi anche la possibilità di controllo a distanza *dell’attività dei lavoratori*» e di quelli «utilizzati dal lavoratore per rendere la prestazione lavorativa».

Pertanto, allo scopo di gestire e mitigare i rischi derivanti dall’utilizzo dei dispositivi informatici (è essenziale assicurare che le informazioni aziendali non siano compromesse), si rende necessario definire specifiche misure di sicurezza.

Il presente regolamento disciplina le condizioni per il corretto utilizzo degli strumenti informatici e/o telematici, anche alla luce degli obblighi previsti in materia di Misure Minime di Sicurezza.

La crescente diffusione di tecnologie informatiche ed il loro utilizzo in ambito lavorativo espone il Comune di Caivano e gli utenti fruitori ad una serie di rischi e di conseguenti responsabilità.

Sebbene principi di diligenza e correttezza siano alla base dell’utilizzo di risorse informatiche, *il Servizio Informatico del Comune di Caivano (in seguito SIC)* ha realizzato questo documento con l’obiettivo di diffondere nozioni fondamentali sulla sicurezza informatica ed evitare che comportamenti non idonei arrechino gravi danni al sistema informativo.

Il regolamento risponde quindi all’esigenza di disciplinare l’utilizzo degli strumenti informatici e contiene indicazioni su quali siano le migliori pratiche da adottare.



COMUNE DI CAIVANO

CITTA' METROPOLITANA DI NAPOLI
Servizio Informatizzazione

1. Indicazioni generali

1.1. Finalità della Policy

Le finalità di questo documento sono:

- garantire e salvaguardare la sicurezza e la privacy degli utenti abilitati *dal Comune di Caivano* (in seguito *Comune*);
- stabilire una policy per la sicurezza e il rispetto della privacy nell'utilizzo delle risorse informatiche comunali con riferimento in particolare alle misure di sicurezza imposte dalle normative per il trattamento di dati personali;
- fornire idonee indicazioni ed istruzioni agli utenti interessati dalle predette misure di sicurezza;
- regolamentare l'utilizzo delle risorse informatiche comunali in modo che siano utilizzate in maniera efficace, produttiva e orientata al raggiungimento degli obiettivi comunali;
- garantire la sicurezza e prevenire il danneggiamento delle risorse informatiche comunali.

1.2. Campo di applicazione

Questa policy si applica:

- a tutte le risorse informatiche di proprietà del *Comune* e/o messe a disposizione nell'ambito del S/C;
- a tutte le operazioni di accesso a informazioni registrate ed archiviate elettronicamente tramite risorse informatiche comunali;
- a tutte le forme di comunicazione operate attraverso la rete comunale e la posta elettronica.

1.3. Destinatari

Il regolamento si applica a tutti i dipendenti a tempo pieno o parziale (senza alcuna distinzione di ruolo e/o livello), collaboratori, consulenti, convenzionati, dipendenti di aziende esterne legate da contratti di fornitura e/o di servizi o altri individui in possesso di specifiche credenziali di autenticazione alla quale è consentito l'utilizzo dell'accesso alle risorse comunali (a prescindere dal tipo di rapporto contrattuale intrattenuto con il *Comune*).

1.4. Entrata in vigore del regolamento e diffusione

Il regolamento entra in vigore con delibera Giunta Comunale su proposta del Responsabile dei Servizi Informatizzati

Con l'entrata in vigore del presente regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presente.

Ai sensi dell'art. 7 Legge n. 300 del 1970, il Comune ai fini dell'esercizio del regolamento, darà adeguata pubblicità mediante invio ai responsabili dei Settori e provvederà alla pubblicazione dello stesso sul sito internet comunale così come indicato dal D.Lgs. n. 33 del 14 marzo 2013.



COMUNE DI CAIVANO

CITTA' METROPOLITANA DI NAPOLI
Servizio Informatizzazione

1.5. Verifiche

Le segnalazioni di eventuali violazioni devono essere repentinamente comunicate al SIC che laddove necessario provvederà ad attivare le idonee procedure di verifica.

Non sono ammesse segnalazioni di violazioni in forma anonima.

Viene comunque tutelato dal Comune il diritto alla privacy degli utenti che comunicassero dette violazioni nei limiti previsti dalla normativa italiana.

1.6. Sanzioni

Poiché in caso di violazioni contrattuali e giuridiche, sia il Comune sia il singolo utente sono potenzialmente perseguibili con sanzioni anche di natura penale, il Comune verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del sistema informativo.

In caso di violazione accertata del presente regolamento, si applica il procedimento disciplinare previsto nel contratto di lavoro e negli accordi sindacali.

Qualsiasi violazione alla normativa italiana vigente da parte degli utenti sarà segnalata alle autorità competenti.



COMUNE DI CAIVANO

CITTA' METROPOLITANA DI NAPOLI
Servizio Informatizzazione

2. Politiche ed utilizzo delle risorse informatiche comunali

2.1 Indicazioni generali

- L'utilizzo delle risorse informatiche comunali e di quelle messe a disposizione dal SIC è riservato agli Utenti espressamente autorizzati dal responsabile del Settore;
- Il responsabile del Settore richiede al SIC l'abilitazione ai servizi informatici e l'accesso alle banche dati necessari a ciascun utente;
- Il responsabile del Settore comunica immediatamente qualsiasi modifica relativa all'organico del servizio che richieda l'attivazione o la sospensione di servizi informatici o autorizzazioni all'accesso alle banche dati (es. cambio di mansioni e/o trasferimento altro servizio);
- le risorse informatiche comunali sono strumenti di lavoro e come tali possono essere utilizzate solo per scopi strettamente lavorativi. Ciò vale sia per le risorse condivise (risorse di rete, stampanti di rete, ecc.), sia per quelle affidate al singolo dipendente (desktop, notebook, periferiche, stampanti, ecc.).
- L'utilizzo di risorse informatiche comunali non deve compromettere la sicurezza e la riservatezza del sistema informativo oltre a non pregiudicare ed ostacolare le attività dell'Amministrazione o essere destinato al perseguimento di interessi privati in contrasto con quelli pubblici;
- le risorse informatiche comunali affidate al singolo utente (es. dispositivi e relativi programmi e/o applicazioni) sono strumenti di lavoro appartenenti al patrimonio comunale e pertanto vanno custoditi in modo appropriato;
- Il furto, il danneggiamento o lo smarrimento di tali strumenti devono essere prontamente segnalati al SIC (e qualora necessario denunciato alle competenti autorità);
- Il dispositivo è assegnato al settore/servizio, in caso di trasferimento dell'utente le risorse informatiche restano al settore di appartenenza salvo esplicita autorizzazione da parte del SIC su richiesta del responsabile del settore;
- le postazioni di lavoro devono essere spente ogni sera prima di lasciare gli uffici.

Casi particolari, in cui ci sia la necessità di lasciare sempre attiva la postazione, devono essere esplicitamente autorizzati dal SIC.

Lasciare un personal computer incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

Qualora l'utente debba allontanarsi dalla propria postazione di lavoro, al fine di prevenire accessi incontrollati da parte di terzi è tenuto ad eseguire una delle seguenti operazioni:

- spegnimento;
- blocco (digitando per es. i tasti CTRL+ALT+CANC);
- disconnessione della postazione di lavoro.

In caso di inattività prolungata la connessione dell'utente potrà essere sospesa e disconnessa in automatico;

i dati sensibili non possono essere salvati nei supporti di memorizzazione locali dei computer a meno di adeguati sistemi di protezione.

Nel caso di computer portatili comunali inoltre:



COMUNE DI CAIVANO

CITTA' METROPOLITANA DI NAPOLI
Servizio Informatizzazione

- L'utente deve custodire con diligenza il dispositivo sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro;
- se il dispositivo è utilizzato all'esterno (convegni, conferenze ecc.), in caso di allontanamento, deve essere custodito in un luogo protetto;
- il dispositivo non deve essere mai lasciato incustodito e sul disco devono essere conservati solo i file strettamente necessari.

2.2 Configurazioni dei dispositivi comunali e collegamento alla rete comunale

- Non è consentita la modifica delle configurazioni impostate dal SIC sul dispositivo;
- Ogni computer comunale deve obbligatoriamente essere collegato alla rete comunale e non può per nessun motivo essere scollegato da tale rete. Casi particolari in cui il computer non debba essere connesso alla rete comunale devono essere esplicitamente autorizzati dal SIC.;
- I computer portatili devono essere collegati alla rete comunale con frequenza almeno mensile al fine di garantire l'aggiornamento di: sistema operativo, antivirus e degli applicativi installati;
- per ragioni di sicurezza non è concesso connettere alla rete comunale stazioni di lavoro private e sistemi di connessione (es. modem, switch, hub ecc.) se non su esplicita e formale autorizzazione del SIC.

2.3 Installazione di hardware e software

Non è permesso :

- l'uso di programmi diversi da quelli distribuiti ufficialmente dal *Comune* su indicazione del SIC, salvo previa autorizzazione esplicita del SIC. L'installazione autonoma di software non autorizzato comporta un grave pericolo di introduzione di virus informatici e/o di alterazione della stabilità delle applicazioni presenti nel sistema informatico comunale;
- l'installazione autonoma di alcun dispositivo di memorizzazione, comunicazione o altro (es. masterizzatori, modem, ecc.), se non con l'autorizzazione esplicita del SIC;
- l'installazione autonoma e/o l'utilizzo di strumenti software e/o hardware atti ad intercettare, falsificare, alterare, criptare o sopprimere il contenuto di comunicazioni e/o di documenti informatici con finalità omissive e fraudolente.

2.4 Supporti di memorizzazione

- Non è consentito l'utilizzo di cd, dvd, chiavette USB, hard disk esterni, ecc. di provenienza ignota o dubbia;
- ogni dispositivo di memorizzazione di provenienza esterna al *Comune* dovrà essere verificato mediante il programma antivirus, presente nel personal computer, prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere consegnato al SIC o a persone delegate;
- non è consentito scaricare file provenienti da Internet oppure contenuti in supporti di memorizzazione che non abbiano una chiara attinenza con la propria prestazione lavorativa;



COMUNE DI CAIVANO

CITTA' METROPOLITANA DI NAPOLI
Servizio Informatizzazione

- i supporti di memorizzazione quali: dvd, chiavette USB, hard disk esterni, ecc. contenenti dati sensibili devono essere ridotti a casi di assoluta necessità e custoditi in archivi chiusi a chiave;
- i supporti di memorizzazione contenenti dati sensibili devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato anche dopo la cancellazione mediante l'utilizzo di specifici strumenti di recupero dati;
- non è consentita la memorizzazione e la diffusione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

2.5 Stampa su stampanti di rete

Si raccomanda agli utenti di prestare la massima attenzione nella stampa soprattutto nel caso si utilizzino delle stampanti di gruppo o accessibili a più persone. Il materiale stampato deve essere immediatamente prelevato per evitare che possa essere visionato da personale non autorizzato.

La stampa di documenti informatici dovrà essere limitata all'attività lavorativa e in ogni caso per documenti per cui esiste l'assoluta necessità di disporre della copia cartacea.

2.6 Scansione da stampante multifunzione con salvataggio su cartella di rete:

- Qualora il file derivante da scansione venga salvato su una cartella condivisa, l'utente si fa carico di spostare il file in una cartella non consultabile da utenti non autorizzati alla visione dei documenti;
- Le scansioni nelle quali vengono salvate nella cartella condivisa vengono periodicamente cancellate automaticamente.
La cancellazione periodica non dispensa tuttavia l'utente dall'obbligo di cancellare/spostare le scansioni eseguite dalla cartella condivisa nel più breve tempo possibile (al fine di non rendere accidentalmente noto a terzi il contenuto dei file scansione).

Si raccomanda di porre la massima attenzione nella scansione di documenti contenenti dati personali e sensibili.

2.7 Credenziali per l'accesso ai dispositivi e alla rete comunale

Per accedere ai dispositivi ed alla rete del *Comune*, l'utente dovrà attenersi al presente regolamento.

- L'accesso ai dispositivi e alla rete comunale avviene mediante un codice di identificazione personale (*iniziale nome cognome*) e una parola chiave segreta (password). La coppia di informazioni prende il nome di credenziali di accesso;
- dovranno essere adottate le necessarie cautele per garantire la segretezza delle credenziali e la diligente custodia dei dispositivi eventualmente in possesso ad uso esclusivo a scopo d'autenticazione (quali ad esempio: smart card.);



COMUNE DI CAIVANO

CITTA' METROPOLITANA DI NAPOLI
Servizio Informatizzazione

- la password di accesso alla rete ha un periodo di validità limitato. A intervalli regolari verrà quindi richiesto all'utente di modificare la password;
- le credenziali di accesso ai dispositivi ed alla rete comunale vengono attribuite dal SIC, all'assunzione del dipendente/inizio del rapporto di collaborazione (ove autorizzato) e devono essere obbligatoriamente modificate al primo accesso;
- le credenziali vengono immediatamente revocate/annulate dal SIC, alla cessazione del rapporto di dipendenza/collaborazione con il *Comune* non appena ne venga a conoscenza (tramite comunicazione da parte del responsabile del settore e/o Ufficio personale);
- le credenziali di accesso ai dispositivi e alla rete attribuite dal SIC, sono modificabili in totale autonomia dall'utente;
- l'utente è tenuto a rispettare le policy per la creazione di password sicure e per la sostituzione programmata stabilita dall'amministratore di sistema;
- l'utente si impegna a non cedere a terzi le proprie credenziali di accesso alla rete, consapevole che la cessione delle stesse consente ad altri l'accesso e l'utilizzo dei relativi servizi, ovvero l'accesso ai dati cui il soggetto è abilitato con conseguenze quali la visualizzazione di informazioni riservate, la distruzione / modifica di dati;
- la responsabilità di qualsiasi azione svolta dopo aver eseguito la procedura di autenticazione sarà attribuita all'utente assegnatario delle credenziali. L'utente è quindi responsabile, sia nei confronti di terzi che del Comune di fatti e atti illeciti, con particolare riferimento all'immissione in rete di contenuti critici o contrari all'ordine pubblico o al buon costume così come definiti dalla giurisprudenza corrente;
- non sono previsti accessi anonimi o di gruppo: laddove questi siano attualmente attivi saranno progressivamente dismessi;
- è assolutamente proibito l'accesso alla rete locale e/o alle applicazioni condivise con nomi utente diversi da quello assegnato;
- l'utente si impegna a modificare tempestivamente la password d'accesso alla rete qualora tale dato sia stato rubato, smarrimento, perso o sia noto a terzi;
- in caso che le credenziali di accesso si siano diffuse in maniera fraudolenta a persone terze (furto, sottrazione illecita, copia non autorizzata, operazioni di pirateria informatica, ecc.) l'utente deve comunicare tempestivamente l'accaduto al SIC;
- nel caso l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediate notizia al SIC;
- il *Comune* si fa garante della custodia dei dati personali forniti dall'utente e si impegna a non rivelarli a terzi, se non a fronte di legittima richiesta da parte di *Autorità Giudiziaria, Autorità di Pubblica Sicurezza e Garante per la Protezione dei Dati Personali*.
- Nel caso che l'Utente digiti per n° 5 volte consecutive la password in maniera errata, il Sistema provvede a bloccare l'utenza. Pertanto, per sbloccare l'utenza, l'utente dovrà contattare il SIC

2.8 Caratteristiche delle credenziali di accesso

Gli utenti sono responsabili della custodia e dell'utilizzo delle proprie credenziali di autenticazione; la password, formata da lettere (maiuscole e minuscole), numeri e/o caratteri speciali, nei limiti consentiti dai sistemi, deve avere le seguenti caratteristiche:

- deve essere di lunghezza non inferiore ad 8 caratteri oppure, nel caso in cui ciò non sia possibile, da un numero di caratteri pari al massimo consentito dal connesso applicativo;



COMUNE DI CAIVANO

CITTA' METROPOLITANA DI NAPOLI
Servizio Informatizzazione

- deve essere composta da caratteri maiuscoli, caratteri minuscoli, numeri e caratteri speciali (es.Y12s@hT!);
- non deve contenere riferimenti agevolmente riconducibili all'Incaricato o ad ambiti noti;
- deve essere obbligatoriamente cambiata al primo utilizzo e successivamente ogni 90 giorni (per quanto concerne le credenziali di dominio esiste un meccanismo di scadenza automatica);
- deve essere diversa dalle ultime 5 password precedentemente utilizzate;
- non deve essere basata su nomi di persone, date di nascita, animali, oggetti o parole ricavabili dal dizionario (anche straniero), o tratta da informazioni personali;
- non deve presentare una sequenza di caratteri identici o in gruppi di caratteri ripetuti;
- non deve essere memorizzata in funzioni di log-in automatico, in un tasto funzionale o nel browser utilizzato per la navigazione Internet;
- deve essere annullata e sostituita con una nuova - per motivate necessità di urgente accesso alle informazioni ed impedimento del titolare delle credenziali - da parte degli amministratori dei servizi o loro delegati. In questo caso essa dovrà essere nuovamente modificata al primo accesso da parte dell'Incaricato.

Qualora le limitazioni tecniche del sistema non permettano la configurazione dello stesso al fine di limitare selettivamente l'utilizzo di password "robuste", sarà onere dell'utilizzatore l'impostazione di password secondo le specifiche in precedenza elencate.

2.9 Unità di rete e cartelle condivise

Per gli utenti del dominio comunale è previsto, previa richiesta al S/C, un sistema di salvataggio dei file su unità di rete.

Le unità di rete si dividono in due categorie:

a. Unità di rete per il salvataggio dei documenti comunali

I documenti salvati in queste unità (server comunali) sono tutelati da perdite mediante accurate procedure di salvataggio.

Il salvataggio su unità di rete è obbligatorio per i dati che richiedono riservatezza (es. dati sensibili, amministrativi, giuridici, economici, ecc.).

La memorizzazione avviene a seconda del grado di riservatezza del documento su cartelle con adeguato livello di condivisione.

I livelli di condivisione/privilegi di lettura e scrittura delle cartelle vengono definiti dal/dai responsabile/i della/e struttura/e proprietaria/e delle cartelle stesse e pertanto dei documenti ivi contenuti;

b. Unità di rete per lo scambio dati (Cartelladiscambio)

Questa unità permette lo scambio di file tra utenti di dominio ma non sono soggetti a procedure di copia di riserva.

Poiché queste unità di rete sono di fatto punto di scambio dove i documenti transitano ma non possono rimanere per lungo periodo il S/C provvederà periodicamente alla cancellazione di tutti i files presenti in tali aree condivise;



COMUNE DI CAIVANO

CITTA' METROPOLITANA DI NAPOLI
Servizio Informatizzazione

- c. entrambe le unità di rete sono aree di condivisione e salvataggio di informazioni inerenti l'attività istituzionale e non possono in alcun modo essere utilizzate per scopi diversi.
- Pertanto qualunque file non legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità;
- d. il S/C si riserva la facoltà di procedere alla rimozione di qualsiasi file o applicazione memorizzata nelle unità di rete qualora ritenuto pericoloso per la sicurezza del sistema; costituisce buona regola la periodica (almeno mensile) cancellazione dagli archivi/cartelle di file obsoleti e/o documenti non più necessari all'attività d'ufficio;
- e. L'utente si impegna a non cedere a terzi le proprie credenziali di accesso alle proprie cartelle condivise consapevole che la cessione delle stesse consente ad altri l'utilizzo/accesso a contenuti riservati e la possibilità di cancellazione e modifica degli stessi.

2.10 Diritti di accesso e controllo remoto

- Per facilitare le operazioni di aggiornamento del software e per garantire la sicurezza dei dispositivi, delle applicazioni e dei dati, il S/C può avvalersi di strumenti di controllo remoto che consentano di compiere le operazioni necessarie attraverso la rete locale;
- l'assistenza tecnica per malfunzionamenti ordinari o diagnosi di sistema attraverso strumenti di controllo remoto deve avvenire solo previa autorizzazione dell'utilizzatore e di norma in presenza dell'utilizzatore stesso;
- in caso di malfunzionamenti straordinari e in situazioni di emergenza, il S/C ha facoltà in qualunque momento di accedere a qualunque sistema informativo comunale per l'espletamento delle proprie funzioni.

Il S/C può in qualunque momento procedere alla rimozione di qualsiasi file o applicazione che riterrà essere pericolosa per la sicurezza, sia sulle postazioni degli utenti che sulle unità di rete.



COMUNE DI CAIVANO

CITTA' METROPOLITANA DI NAPOLI
Servizio Informatizzazione

3. Utilizzo della rete Internet e dei relativi servizi

Le regole di seguito specificate sono adottate anche ai sensi delle "Linee guida del Garante per posta elettronica e internet" pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007.

Ciascun Utente si deve attenere alle seguenti regole di utilizzo della rete Internet e dei relativi servizi:

3.1. Regole di utilizzo di internet nelle sedi comunali

- L'abilitazione alla navigazione su internet deve essere accordata dal responsabile del trattamento che invia richiesta formale al SIC tramite invio a: ced@comune.caivano.na.it;
- qualora l'utente non fosse stato abilitato alla navigazione in internet è fatto divieto assoluto di connettersi autonomamente alla rete internet;
- è tassativamente proibito l'utilizzo di sistemi di connessione quali modem dial-up, chiavette internet e condivisione di connessione con dispositivi mobili (hotspot e tethering), collegamento a reti wi-fi diversa da quella comunale;
- è vietato modificare le impostazioni di connessione stabilite dal SIC per le postazioni comunali (firewall, IP, proxy ecc.);
- È ammessa solo la navigazione in siti considerati correlati con la prestazione lavorativa. L'accesso è consentito dai sistemi di filtraggio implementati dall'Ente con le sue policy di sicurezza, ad es. i siti istituzionali, i siti degli Enti locali, di fornitori e partner dell'Ente.
- È vietato compiere azioni che siano potenzialmente in grado di arrecare danno all'Ente (sovraccarico della rete; introduzione di virus informatici), ad esempio, il download o l'upload di file audio e/o video, l'uso di servizi di rete con finalità ludiche o, comunque, estranee all'attività lavorativa;
- È vietato a chiunque il download di qualunque tipo di software gratuito (freeware) o shareware prelevato da siti Internet, se non espressamente autorizzato dal SIC;
- L'Ente si riserva di bloccare l'accesso a siti "a rischio" attraverso l'utilizzo di blacklist pubbliche in continuo aggiornamento, e di predisporre filtri, basati su sistemi euristici di valutazione del livello di sicurezza dei siti web remoti, tali da prevenire operazioni potenzialmente pericolose o comportamenti impropri. In caso di blocco accidentale di siti di interesse dell'Ente, contattare il SIC per uno sblocco selettivo (ced@comune.caivano.na.it);
- Nel caso in cui, per ragioni di servizio, si necessiti di una navigazione libera da filtri, è necessario richiedere lo sblocco mediante una mail indirizzata a ced@comune.caivano.na.it, ed in copia al Responsabile di Settore, nella quale siano indicati chiaramente: motivo della richiesta, utente e postazione da cui effettuare la navigazione libera, ed eventualmente intervallo di tempo richiesto per completare l'attività;



COMUNE DI CAIVANO

CITTA' METROPOLITANA DI NAPOLI
Servizio Informatizzazione

- È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo i casi direttamente autorizzati dall'Ente o comunque nell'ambito di un procedimento amministrativo che preveda dei movimenti finanziari;
- qualsiasi divulgazione di informazioni nella rete internet relative a strutture e/o attività comunali dovrà rispettare specifici regolamenti comunali in materia;
- gli utenti sono invitati a limitare il rilascio di informazioni personali durante la navigazione via Web.
- L'utente è tenuto nel corso della navigazione a leggere con attenzione qualsiasi finestra, pop up o avvertenza prima di proseguire nella navigazione e in particolare prima di accettare delle condizioni contrattuali o di aderire a delle iniziative online;
- per ragioni di sicurezza non è concesso scaricare software dalla rete. Eventuali necessità dovranno essere appositamente concordate con il SIC che provvederà ad eseguire fisicamente lo scarico da una stazione protetta e ad applicare le misure antivirus relative. Il software scaricato sarà poi installato dal personale autorizzato al richiedente;
- è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
- il *Servizio Informatico*, su autorizzazione del Segretario Comunale, ha facoltà di porre limiti alla navigazione internet escludendo dalla navigazioni siti non attinenti agli scopi comunali;
- è vietato l'utilizzo di internet a scopi personali non attinenti l'attività istituzionale quali a titolo d'esempio: la partecipazione a forum, l'utilizzo di chat-line, bacheche elettroniche e servizi di rete sociale, la registrazione in guest-book anche utilizzando pseudonimi (nickname), l'adesione a servizi gratuiti di social networking e microblogging, remote banking, acquisti online e simili.
- Si informa che l'Ente non effettua la memorizzazione sistematica delle pagine web visualizzate dal singolo utente, né controlla con sistemi automatici i dati di navigazione dello stesso.
Si informa tuttavia che al fine di garantire il Servizio Internet e la sicurezza dei Sistemi Informativi, nonché per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente, l'Ente registra per 7 giorni i dati di navigazione (file di log riferiti al traffico web) con modalità inizialmente volte a precludere l'immediata e diretta identificazione di Utenti, mediante opportune aggregazioni.
Le informazioni così raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 679/16 "GDPR".



COMUNE DI CAIVANO

CITTA' METROPOLITANA DI NAPOLI
Servizio Informatizzazione

4. Posta elettronica

Le regole di seguito specificate sono adottate anche ai sensi delle "Linee guida del Garante per posta elettronica e internet" pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007.

Ciascun Utente si deve attenere alle seguenti regole di utilizzo dell'indirizzo di posta elettronica.

4.1. Casella di posta elettronica comunale

- All'atto dell'assunzione/inizio di collaborazione viene assegnata una casella di posta elettronica comunale nominativa al dipendente/collaboratore (ove autorizzato), nel dominio dell'Ente (comune.caivano.na.it), generalmente coerente con il modello `iniziale.cognome`; l'utilizzo dell'e-mail deve essere limitato esclusivamente a scopi lavorativi, ed è assolutamente vietato ogni utilizzo di tipo privato. L'utente a cui è assegnata una casella di posta elettronica è responsabile del corretto utilizzo della stessa e di conservare e modificare frequentemente la password secondo le medesime indicazioni fornite per la gestione dell'account di accesso alle PdL.

L'Ente fornisce, altresì, delle caselle di posta elettronica associate a ciascuna unità organizzativa, ufficio o gruppo di Lavoro (es. ufficio@comune.caivano.na.it), il cui utilizzo è da preferire rispetto alle e-mail nominative qualora le comunicazioni siano di interesse collettivo: questo per evitare che degli utenti singoli mantengano l'esclusività sui dati dell'Ente.

Si ricorda altresì che tutta la corrispondenza con cittadini, imprese ed altra amministrazione relativa a procedimenti amministrativi è opportuno transiti attraverso il protocollo dell'Ente (protocollo.caivano@asmepec.it) e venga **gestita con i canali telematici ufficiali.**

- all'atto della cessazione del rapporto di dipendenza/collaborazione con il *Comune* la casella mail viene bloccata e/o cancellata;
- l'amministratore di sistema per comprovati motivi può revocare/cancellare la casella di posta elettronica comunale nominativa di un dipendente / collaboratore;

4.2. Credenziali per l'accesso alla casella di posta elettronica

- L'accesso alla casella di posta elettronica comunale avviene mediante un codice di identificazione personale e una parola chiave segreta. La coppia di informazioni prende il nome di credenziali di accesso;
- le credenziali di accesso alla casella di posta elettronica vengono attribuite dal all'assunzione del dipendente/inizio del rapporto di collaborazione (ove autorizzato) e devono essere obbligatoriamente modificate la primo accesso;
- le credenziali vengono immediatamente revocate/annullate dal SIC alla cessazione del rapporto di dipendenza/collaborazione con l'*Comune* non appena ne venga a conoscenza (tramite comunicazione da parte del responsabile al trattamento e/o uff. personale);
- le credenziali di accesso attribuite dal SIC, sono modificabili in totale autonomia dall'utente;
- l'utente è tenuto a rispettare le policy per la creazione di password sicure e per la sostituzione programmata stabilita dall'amministratore di sistema;
- l'utente si impegna a non cedere a terzi le proprie credenziali di accesso alla casella di posta elettronica consapevole che la cessione delle stesse consente ad



COMUNE DI CAIVANO

CITTA' METROPOLITANA DI NAPOLI
Servizio Informatizzazione

- altri l'accesso ai servizi di posta con possibilità di inviare e ricevere mail a nome dell'utente abilitato;
- la responsabilità di qualsiasi azione svolta dopo aver eseguito la procedura di autenticazione alla casella di posta elettronica sarà attribuita all'utente assegnatario delle credenziali. L'utente è quindi responsabile, sia nei confronti di terzi che del Comune, di fatti e atti illeciti. Quanto sopra vale per le caselle di posta elettronica istituzionali condivise alle quali si accede per tramite del proprio account;
 - qualora l'utente debba allontanarsi dalla propria postazione di lavoro, al fine di prevenire accessi incontrollati da parte di terzi è tenuto ad uscire dalla casella di posta elettronica;
 - è assolutamente proibito l'accesso a caselle di posta comunali diverse da quella/e assegnate;
 - l'utente si impegna a modificare tempestivamente la password d'accesso alla casella di posta qualora tale dato sia stato rubato, smarrito o sia noto terzi;
 - in caso il dato si sia diffuso in maniera fraudolenta a persone terze (furto, sottrazione illecita, copia non autorizzata, operazioni di pirateria informatica, ecc.) l'utente deve comunicare tempestivamente l'accaduto al SIC;
 - nel caso l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia al SIC;

4.3. Utilizzi consentiti della posta elettronica

La casella di posta è uno strumento di lavoro assegnato all'atto dell'assunzione dal SIC

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

- È fatto divieto di inviare/ricevere posta elettronica su caselle diverse da quelle assegnate dal SIC all'utente;
- non è consentito l'utilizzo della posta elettronica per motivi non attinenti allo svolgimento delle mansioni assegnate. In particolare è fatto divieto di utilizzare le caselle di posta elettronica comunale per l'invio di messaggi personali;
- è fatto divieto di utilizzare le risorse informatiche per la comunicazione elettronica in modo anonimo o modificando la reale identità del mittente;
- la posta elettronica diretta all'esterno della rete informatica comunale può essere intercettata da estranei, e dunque, non deve essere usata per inviare documenti di lavoro "strettamente riservati";
- l'utente è tenuto a seguire attentamente le disposizioni date dal SIC riguardanti la protezione da virus e da altri software che possano diffondersi via mail;
- è vietato l'utilizzo di tecniche di "mail spamming" cioè l'invio massivo di comunicazioni a liste di comunicazioni extra comunali e/o di azioni equivalenti;
- nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente:
 1. sospendere ogni elaborazione in corso senza spegnere il computer;
 2. segnalare l'accaduto al SIC.;
- Allo scopo di garantire sicurezza alla rete dell'Ente, evitare di aprire messaggi di posta in arrivo da mittenti di cui non si conosce l'identità, con i quali non sussiste alcun rapporto lavorativo o con contenuto sospetto o insolito, oppure che contengano allegati di tipo *.exe, *.com, *.vbs, *.htm, *.scr, *.bat, *.js, *.xlse, *.xlsx e *.pif. È necessario porre molta attenzione, inoltre, alla credibilità del messaggio e del mittente per evitare casi di phishing, frodi informatiche,



COMUNE DI CAIVANO

CITTA' METROPOLITANA DI NAPOLI
Servizio Informatizzazione

od installazione involontaria di software malevolo. In qualunque situazione di incertezza, prima di eseguire qualsiasi azione, contattare il SIC per una valutazione dei singoli casi.

- Non é consentito diffondere messaggi del tipo "catena di S.Antonio" o di tipologia simile, anche se il contenuto sembra meritevole di attenzione; in particolare gli appelli di solidarietà e i messaggi che informano dell'esistenza di nuovi virus. In generale è vietata la diffusione di messaggi pubblicitari di prodotti di qualsiasi tipo.
- Nel caso fosse necessario inviare allegati "pesanti" (oltre i 10MB) è opportuno ricorrere prima alla compressione dei file originali in un archivio di formato .zip o equivalente. Nel caso di allegati ancora più voluminosi è necessario rivolgersi al SIC per la valutazione delle soluzioni.

Nel caso in cui fosse necessario inviare a destinatari esterni messaggi contenenti allegati con dati personali o dati personali sensibili, è obbligatorio che questi allegati vengano preventivamente resi inintelligibili attraverso crittazione con apposito software (archiviazione e compressione con password). La password di crittazione deve essere comunicata al destinatario attraverso un canale diverso dalla mail (ad esempio per lettera o per telefono) e mai assieme ai dati crittati. Tutte le informazioni dell'Ente, i dati personali e/o sensibili di competenza dell'Ente possono essere inviati soltanto a destinatari - persone o Enti – qualificati e competenti, e nell'ambito di un procedimento amministrativo, preferendo allo scopo i canali di comunicazione istituzionali.

- Non è consentito l'invio automatico di e-mail all'indirizzo e-mail privato (attivando per esempio un "inoltrato" automatico delle e-mail entranti), anche durante i periodi di assenza (es. ferie, malattia, infortunio ecc.). In questa ultima ipotesi, è preferibile utilizzare l'inoltrato automatico ad altre caselle dell'Ente e/o un messaggio di autoreply "Fuori Ufficio/Out of Office", facendo menzione di chi, all'interno dell'Ente, assumerà le mansioni durante l'assenza, oppure indicando un indirizzo di mail alternativo, preferibilmente di tipo collettivo, tipo ufficioX@comune.caivano.na.it.

In caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, qualora non fosse possibile attivare la funzione autoreply o l'inoltrato automatico su altre caselle dell'Ente e si debba conoscere il contenuto dei messaggi di posta elettronica, il titolare della casella di posta ha la facoltà di delegare un altro dipendente (fiduciario) per verificare il contenuto di messaggi e per inoltrare al Responsabile di Settore quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Sarà compito dello stesso assicurarsi che sia redatto un verbale attestante quanto avvenuto e che sia informato il lavoratore interessato alla prima occasione utile. Si ricorda comunque della possibilità di accesso alla propria casella di posta elettronica da qualsiasi dispositivo connesso ad internet e dotato di browser.

- La diffusione massiva di messaggi di posta elettronica deve essere effettuata esclusivamente per motivi inerenti il servizio, possibilmente su autorizzazione del responsabile di Settore competente. Per evitare che le eventuali risposte siano inoltrate a tutti, generando traffico eccessivo ed indesiderato, i destinatari dovranno essere messi in copia nascosta (Bcc o Ccn), se la tipologia del messaggio lo consente. Si ricorda che vi sono comunque dei limiti all'invio massivo di messaggi dalla casella di posta e che è possibile utilizzare il servizio di invio newsletter, più idoneo a gestire comunicazioni/avvisi/inviti ad una pluralità di soggetti.
È vietato inviare posta elettronica in nome e per conto di un altro utente, salvo sua espressa autorizzazione.



COMUNE DI CAIVANO

CITTA' METROPOLITANA DI NAPOLI
Servizio Informatizzazione

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

Si ricorda che non vengono effettuati backup periodici della posta elettronica personale, pertanto è compito del singolo utente, se lo ritenesse necessario, gestire in autonomia queste attività.

La posta elettronica può essere gestita sia dalla PdL in dotazione che da qualsiasi dispositivo connesso ad internet, utilizzando il portale raggiungibile all'indirizzo

<https://webmail.aruba.it>

e le credenziali personali della casella.

Si informa che le comunicazioni, anche elettroniche, ed i documenti elettronici allegati possono avere rilevanza procedimentale e pertanto devono essere conservate per la durata prevista dalla normativa vigente.

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

Si informa che, in caso di cessazione del rapporto lavorativo, la mail dell'Ente affidata all'incaricato verrà bloccata.

4.4. Contenuto dei messaggi

- Non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- gli utenti devono prestare attenzione nell'invio di messaggi elettronici affinché non siano inserite inconsapevolmente delle informazioni su credenziali utilizzate in altre applicazioni;



COMUNE DI CAIVANO

CITTA' METROPOLITANA DI NAPOLI
Servizio Informatizzazione

- gli utenti sono invitati a nominare correttamente i nomi dei file allegati alle e-mail, specificando, nel caso si procedesse ad inviare documenti soggetti a modifiche e revisioni, la versione corrente del file con dei numeri progressivi;
- Gli utenti sono invitati a prestare attenzione nell'utilizzo della funzione "Rispondi" e "Rispondi a tutti" nel caso il messaggio originario sia stato inviato ad un numero elevato di destinatari.

4.5. Altre istruzioni riguardanti la posta elettronica

- Gli utenti sono invitati a leggere quotidianamente la posta elettronica e a rispondere in tempi ragionevoli alle e-mail ricevute;
- Gli utenti sono invitati ad inviare allegati in formati comuni (MSOffice, Libre Office, OpenOffice ecc.) possibilmente senza funzioni macro. L'incapacità per il destinatario di aprire file con estensioni poco comuni potrebbe comportare la cancellazione del messaggio (scambiato per un allegato dannoso);
- Gli utenti che hanno selezionato l'opzione di completamento automatico dell'indirizzo devono prestare molta attenzione nella selezione dei destinatari;
- Gli utenti devono periodicamente cancellare o organizzare in opportune cartelle la posta già letta.
Una quantità troppo elevata di e-mail nella cartella predefinita di arrivo può compromettere sensibilmente la stabilità del programma di posta;
- Gli utenti devono sempre indicare con chiarezza nel campo oggetto, l'argomento del proprio messaggio;
- E' possibile richiedere una ricevuta di lettura / ricevimento della propria mail. A tale ricevuta va tuttavia assegnata un'importanza relativa;
- La conferma della ricezione avviene per opera del mail server centrale e non del destinatario ultimo del messaggio. Non sempre il destinatario conferma la lettura di un messaggio o utilizza sistemi di posta elettronica compatibili, pertanto non vi è certezza sullo stato di ricezione del messaggio;
- Gli utenti sono invitati a porre attenzione a mail provenienti da mittenti sospetti, mail il cui messaggio riporti errori di ortografia o lessicali e/o contenenti allegati inconsueti non accompagnati da alcun messaggio di testo;
- Si raccomanda di prevedere, con la funzione di inserimento automatico della firma in calce all'e-mail, la seguente avvertenza sulla privacy e sulla confidenzialità dei messaggi inviati: *"Questo messaggio è di carattere riservato ed è indirizzato esclusivamente al destinatario specificato. L'accesso, la divulgazione, la copia o la diffusione sono vietate a chiunque altro ai sensi delle normative vigenti, e possono costituire una violazione penale. In caso di errore nella ricezione, il ricevente è tenuto a cancellare immediatamente il messaggio, dandone conferma al mittente a mezzo e-mail."*

Terminologie e abbreviazioni

Nel presente testo verranno utilizzati i seguenti termini:

- **amministratore di sistema:** persona che a qualunque titolo (dipendenti del Servizio Informatico Comunale o consulente esterno al Servizio Informatizzazione) ricopre uno dei ruoli sotto indicati relativamente a sistemi informatici del Comune":
 - System Administrator: il ruolo contempla lo svolgimento di attività di amministrazione (installazione, configurazione, risoluzione malfunzionamenti, salvataggi, protezioni, ecc...) su sistemi operativi e software di base e d'ambiente;
 - Network Administrator: il ruolo contempla lo svolgimento di attività di amministrazione (installazione, configurazione, risoluzione malfunzionamenti, ecc...) sulle componenti di una rete telematica (cablaggi, apparati di rete di varia natura);
 - Database Administrator: il ruolo contempla lo svolgimento di attività di amministrazione (installazione, configurazione, risoluzione malfunzionamenti, ecc...) sui sistemi di gestione di basi di dati;
 - Software Administrator: il ruolo contempla lo svolgimento di attività di amministrazione (configurazione, manutenzione, attribuzione di privilegi, ecc...) specifiche nel contesto di un'applicazione adibita al trattamento dei dati personali e/o sensibili.

La designazione degli amministratori di sistema è individuale e deve indicare l'ambito di operatività. La designazione è effettuata dal Responsabile del Servizio Informatizzazione

- **comunicazione elettronica:** qualsiasi comunicazione creata, inviata, inoltrata, trasmessa, archiviata, copiata, scaricata, mostrata, vista o stampata da uno o più sistemi o servizi di comunicazione elettronica;
- **e-mail:** posta elettronica per lo scambio di messaggi e di documenti;
- **incaricato al trattamento:** ciascun utente delle risorse informatiche che effettui trattamenti di dati personali;
- **policy o regolamento:** documento che ha come oggetto la regolamentazione di una determinata funzione comunale. Può inoltre contenere delle linee guida e dei suggerimenti per una migliore fruizione dei servizi comunali;
- **postazione di lavoro:** calcolatore/computer collegato alla rete comunale tramite il quale l'utente può accedere ai servizi di rete;
- **remote banking:** servizi automatizzati che consentono al cliente di collegarsi da remoto, utilizzando un computer, all'elaboratore della banca presso la quale intrattengono il rapporto di conto Corrente;
- **risorse informatiche comunali:** qualsiasi combinazione di apparati tecnologici *del Comune*, hardware o software utilizzati per le comunicazioni elettroniche ed elaborazione dei dati;
- **S.I.C:** la struttura organizzativa che all'interno del *Comune* si occupa della gestione operativa delle risorse informatiche comunali;
- **sito internet/intranet:** è l'insieme dei file realizzati secondo lo standard HTML destinati ad essere installati su un server web e visibili dagli utenti;
- **situazione d'emergenza:** circostanza nella quale il venir meno di un'azione può provocare un serio pregiudizio a persone o cose, comportare il danneggiamento o la scomparsa di dati o impedire la verifica di una grave responsabilità del *Comune* o di qualche dipendente;
- **spam:** è l'invio di grandi quantità di messaggi. Può essere messo in atto attraverso qualunque media, ma il più usato è Internet, attraverso l'e-mail;
- **supporti di memorizzazione:** dischetti, cd, dvd, chiavette USB, hard disk esterni, ecc.
- **utente:** dipendenti a tempo pieno o parziale, collaboratori, consulenti, dipendenti di aziende esterne legate da contratti di fornitura di servizi o altri individui in possesso di specifiche credenziali di autenticazione alla quale è consentito l'utilizzo dell'accesso alle risorse comunali



COMUNE DI CAIVANO

CITTA' METROPOLITANA DI NAPOLI

VERBALE DI DELIBERAZIONE DELLA GIUNTA COMUNALE

N° 262 del 30/11/2022

OGGETTO: REGOLAMENTO PER UTILIZZO STRUMENTI INFORMATICI DA PARTE DEGLI UFFICI COMUNALI - ADOZIONE

L'anno duemilaventidue addi trenta del mese di Novembre alle ore 10:01, nella sede del Comune di Caivano, previo esaurimento delle formalità prescritte dalla Legge e dallo Statuto, si è riunita sotto la presidenza del Il Sindaco Vincenzo Falco la Giunta Comunale. Partecipa all'adunanza ed è incaricato della redazione del presente verbale il Segretario Generale Dott. Carmine Testa.

Intervengono i Signori:

N°	Qualifica	Nome	Presente	Assente
<u>1</u>	FALCO VINCENZO	Sindaco	X	
<u>2</u>	ANTONELLI TONIA	Vice Sindaco	X	
<u>3</u>	BERVICATO MARIA GIUSEPPINA	Assessore	X	
<u>4</u>	PELUSO CARMINE	Assessore	X	
<u>5</u>	MENNILLO PASQUALE	Assessore	X	
<u>6</u>	ARIEMMA PIERINA	Assessore	X	
<u>7</u>	DELLA ROCCA ARCANGELO	Assessore	X	
<u>8</u>	DONESI MARIA	Assessore	X	

PRESENTI: 8

ASSENTI: 0

Il Presidente, riconosciuta legale l'adunanza dichiara aperta la seduta ed invita la Giunta Comunale a trattare il seguente argomento :

OGGETTO: REGOLAMENTO PER UTILIZZO STRUMENTI INFORMATICI DA PARTE DEGLI UFFICI COMUNALI - ADOZIONE

Proposta alla Giunta Municipale

IL RESPONSABILE DEI SISTEMI INFORMATIVI

Premesso che:

a fronte dei notevoli vantaggi delle nuove tecnologie, l'utilizzo improprio degli strumenti informatici comporta seri e gravi rischi sia per il datore di lavoro (per abusi perpetrati dai dipendenti per mezzo della strumentazione in dotazione), che per i lavoratori (per potenziali controlli occulti e ingiustificatamente invasivi da parte del datore di lavoro per mezzo della strumentazione in dotazione);

al fine di garantire massima tutela per entrambe le parti, l'Ente ritiene indispensabile la definizione di un regolamento disciplinante le regole generali per il corretto utilizzo delle dotazioni informatiche da parte del personale dell'Ente (dirigenti e personale delle categorie, a tempo indeterminato e determinato), nonché dei collaboratori che abbiano accesso alle dotazioni informatiche dell'Ente;

secondo l'interpretazione prevalente in materia, tale regolamento va ricondotto alle disposizioni di cui all'art. 4 della Legge n. 300/1970 (Statuto dei Lavoratori);

alla fonte normativa, si aggiunge il provvedimento del Garante per la protezione dei dati personali, recante "Linee guida per posta elettronica e internet", assunto con deliberazione n.13 del 1° marzo 2007, che impone ai datori di lavoro l'onere di adottare specifiche modalità di utilizzo della posta elettronica e di internet, indicando con chiarezza le modalità di uso degli strumenti messi a disposizione, e se, e in che misura e con quali modalità, vengono effettuati controlli;

in linea con le disposizioni del Garante sopra citate, e quale precisa scelta da parte dell'Ente, i principi fondamentali dell'atto regolamentare, nonché le eventuali misure organizzative che verranno in futuro adottate nel rispetto delle norme, sono quelli della prevenzione degli abusi, anziché della loro repressione, della minimizzazione dell'uso di dati eventualmente riferibili ai lavoratori, e, infine, dal rispetto del divieto di esercitare forme di attività di controllo a distanza dell'attività dei lavoratori.

Visto il testo del Regolamento sull'utilizzo degli strumenti informatici, che si allega sub A) al presente atto, per formarne parte integrante e sostanziale;

Visto il D.Lgs. n. 67/2000;
Visto il D.Lgs. n. 165/2001;

SI PROPONE

- 1) di adottare il “*Regolamento sull’utilizzo degli strumenti informatici da parte degli uffici comunali*”, allegato alla presente, per costituirne parte integrante e sostanziale;
- 2) di dare mandato ai Responsabili di Posizioni Organizzative affinché venga data ampia diffusione al Regolamento.

Il Responsabile Settore Ragioneria e Finanze
(Dott. Gennaro Sirico)

LA GIUNTA MUNICIPALE

Vista la proposta di deliberazione come sopra articolata;
Visti i pareri favorevoli espressi dal competente funzionario dell’Ente in ordine alla regolarità tecnica e contabile, ai sensi dell’art.49 del DLgs.n.267/00;
Ad unanimità di voti favorevoli espressi nei modi e forme di legge;

DELIBERA

-di approvare la su estesa proposta di deliberazione come sopra articolata che nel presente dispositivo si intende integralmente riportata anche se non materialmente trascritta;

Dichiarare il presente atto immediatamente eseguibile, ai sensi dell’art.134 del DLgs.n.267/00 a seguito di separata ed unanime votazione favorevole dei presenti.

Letto, confermato e sottoscritto

IL Il Sindaco
Vincenzo Falco

(atto sottoscritto digitalmente)

IL Segretario Generale
Dott. Carmine Testa