



COMUNE DI COSTA MASNAGA

Provincia di Lecco

Regolamento di utilizzo del Sistema Informatico Comunale

Approvate con Deliberazione di Giunta Comunale n. 83 del 7.10.2022

Articolo 1 - Riferimenti

I riferimenti normativi del presente regolamento sono i seguenti:

- Regolamento (UE) n. 2016/679, General Data Protection Regulation (GDPR)
- Provvedimento a carattere generale del Garante del 27 novembre 2008 dal titolo "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", pubblicato sulla G.U. n. 300 del 24 dicembre 2008;

Il regolamento tiene inoltre conto di quanto disposto dal "Modulo di implementazione" allegato alla Circolare 18 aprile 2017, n. 2/2017, recante «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)

Articolo 2 - Definizioni

Ai fini dell'applicazione del presente regolamento deve intendersi per:

Sistema Informatico Comunale (di seguito S.I.C.): l'insieme degli strumenti tecnologici utilizzati dal Comune per il trattamento e la conservazione delle informazioni, composto dalle singole postazioni di lavoro, da elementi hardware (server di rete, stampanti, periferiche, ecc.), software (programmi informatici di base e applicativi, database, ecc.) e reti telematiche.

Titolare del Trattamento dei dati personali (Titolare): persona fisica cui competono le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali ed agli strumenti utilizzati, ivi compreso il profilo della sicurezza. Per il Comune di Costa Masnaga, il Legale Rappresentante dell'Ente, individuato nel Sindaco *pro-tempore*.

Amministratore di Sistema (AdS): figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione dati, all'amministrazione di basi di dati, di reti, di apparati di sicurezza e di sistemi software complessi.

Utente: persona che a qualsiasi titolo accede, anche in forma parziale o per limitati periodi di tempo, al S.I.C.

Articolo 3 - Informazioni e norme generali

Gli Utenti del S.I.C. sono formalmente autorizzati dall'Amministrazione e tecnicamente abilitati dal AdS, non è consentito alcun accesso anonimo o non autorizzato.

Ogni utente è tenuto ad osservare il presente regolamento al fine di preservare la funzionalità e la sicurezza del sistema stesso e delle informazioni gestite e conservate, a tal fine ogni utente riceve copia integrale del presente documento e firma l'allegato modulo per presa visione e accettazione.

Gli strumenti informatici possono essere utilizzati unicamente per gli scopi definiti dall'Amministrazione.

Articolo 4 - Norme tecniche

Postazioni di lavoro

Ogni postazione di lavoro viene installata con una configurazione adatta alle specifiche esigenze delle varie realtà lavorative, concordata dai Responsabili di servizio con l'AdS.

La postazione si compone di:

- dotazione hardware e software
- impostazioni utente (salvaschermo, memorizzazione password, ecc.)
- autorizzazione per l'accesso a cartelle condivise e software applicativi

Qualsiasi variazione alla configurazione della postazione di lavoro (ad esempio l'installazione di nuovi software o la rimozione o aggiornamento di quelli presenti, l'utilizzo di USB drive o altri supporti informatici, la modifica delle impostazioni utente, ecc.) deve essere preventivamente autorizzata dal Responsabile di servizio e concordata con l'AdS.

Non è consentito il collegamento al S.I.C. di apparecchiature non di proprietà dell'Amministrazione, salvo specifica autorizzazione del AdS.

Credenziali utente

Ciascun utente del S.I.C. si connette alla rete, alle piattaforme software e alla posta elettronica, tramite autenticazione univoca personale. L'utente è tenuto a custodire e garantire la segretezza della parola chiave e a sostituirla almeno ogni sei mesi.

Le password sono modificabili da tutti gli utenti in qualsiasi momento tramite apposita procedura, specifica di ogni contesto applicativo.

I requisiti minimi di complessità delle password sono:

- redazione con caratteri maiuscoli e minuscoli
- composizione con inclusione di lettere, numeri e simboli o segni di punteggiatura
- numero caratteri non inferiori a 8
- password non agevolmente riconducibile all'identità del soggetto che la gestisce

Il Titolare del Trattamento dati personali può richiedere agli AdS la disponibilità di dati o strumenti elettronici assegnati ad un utente in caso di sua prolungata assenza o di impedimento. Ciò avviene attraverso la sostituzione della password effettuata dal AdS che la comunica al Titolare. L'AdS comunica tempestivamente e per iscritto all'utente l'avvenuto cambio delle credenziali di accesso e le motivazioni.

Gestione dei dati

La rete interna, istituita appositamente per permettere collegamenti funzionali tra gli utenti, non può esser utilizzata per scopi diversi da quelli ai quali è destinata.

Le cartelle di rete sono sottoposte a procedure di backup e controllo degli accessi e sono l'unico supporto sicuro sul quale memorizzare i documenti elettronici. L'utilizzo da parte degli utenti di qualsiasi altro supporto di memorizzazione (ad esempio le cartelle locali del personal computer) non garantisce la sicurezza del dato in caso di guasti hardware, sovrascritture o cancellazioni accidentali, attacchi informatici di virus o altri software malevoli.

Qualsiasi file estraneo all'attività lavorativa, se non espressamente autorizzato, non può, nemmeno in via transitoria, essere salvato nelle cartelle di rete.

Tutti i file di provenienza incerta o comunque esterna (Internet, posta elettronica, supporti rimovibili), ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo antivirus.

È vietata la cifratura di documenti effettuata autonomamente dall'utente se non concordata e autorizzata dal ADS.

Utilizzo rete Internet

L'accesso a Internet è possibile da qualsiasi postazione connessa alla rete e costituisce parte integrante della dotazione informatica di ogni utente.

Non è consentito l'accesso a siti, social network o qualsiasi altro tipo di risorsa on-line, per scopi non inerenti alla propria attività lavorativa, salvo autorizzazione concordata con l'Amministrazione Comunale.

L'Amministrazione Comunale può inoltre avvalersi di sistemi in grado di documentare il traffico internet generato dalle stazioni di lavoro. Tali informazioni sono raccolte unicamente allo scopo di verificare ex-post utilizzi illeciti del collegamento ad Internet e il loro accesso è consentito unicamente al Titolare del trattamento dati personali e si effettuerà unicamente nei modi previsti dalla legge ed in particolare secondo principi di gradualità dei controlli, pertinenza e non eccedenza.

Utilizzo posta elettronica

Tutte le caselle appartenenti al dominio istituzionale, comprese pertanto anche quelle nominali, sono di esclusiva proprietà dell'Amministrazione Comunale e il loro utilizzo è autorizzato solo per esigenze di servizio.

Lo strumento della posta elettronica non sostituisce altri sistemi più idonei per l'interscambio di documenti; pertanto, l'invio di allegati è consentito solo per file con dimensioni contenute (fino a un massimo di 25 Mb).

In caso di assenza programmata o prolungata, ogni utente dispone di apposite funzioni automatiche di sistema che consentono di inviare messaggi di risposta o inoltrare la posta verso differenti indirizzi.

Portale Internet comunale

Gli utenti autorizzati possono pubblicare pagine informative e modulistica sul portale Internet comunale, utilizzando gli strumenti di redazione messi a disposizione dal S.I.C.

Ogni utente è responsabile dei contenuti da esso pubblicati ed è tenuto a verificarli prima dell'effettiva pubblicazione, al fine di garantire la tutela dell'Ente.

Protezione antivirus

Ogni utente è tenuto a tenere comportamenti tali da ridurre il rischio di attacco al S.I.C. da parte di virus o di ogni altro software malevolo che operi con lo scopo di superare le difese di sicurezza del sistema stesso.

A tal fine, ogni utente è tenuto a:

- evitare tassativamente l'apertura di file allegati ad e-mail provenienti da utenti sconosciuti o contenenti messaggi sospetti
- segnalare tempestivamente al AdS eventuali avvisi di rischio ricevuti dal software antivirus installato o altre anomalie di funzionamento del sistema
- evitare la navigazione Internet su siti non istituzionali o la cui affidabilità non è accertabile

- evitare l'utilizzo di dispositivi rimovibili (USB drive, CD/DVD, floppy disk o simili) personali o non autorizzati dal AdS
- controllare, mediante il software antivirus, il contenuto di supporti rimovibili autorizzati prima di ogni utilizzo

Accesso ad archivi contenenti dati personali

Il Comune di Costa Masnaga, per perseguire le proprie finalità istituzionali, gestisce archivi contenenti dati personali tutelati dalla normativa in materia di Privacy.

L'accesso agli archivi contenenti dati personali (comuni e/o sensibili) è consentito esclusivamente agli utenti autorizzati, identificati tramite le proprie credenziali di accesso al sistema.

Ogni utente è tenuto a non allontanarsi dal proprio posto di lavoro senza aver prima chiuso la propria sessione di lavoro o bloccato in altro modo l'accesso non autorizzato al proprio sistema.

Utilizzo dei materiali di consumo

L'utilizzo delle stampanti e dei materiali di consumo in genere (carta, inchiostro, toner, floppy disk, CD, DVD) è riservato esclusivamente a funzioni inerenti all'attività lavorativa.

Devono essere evitati in ogni modo sprechi dei suddetti materiali o utilizzi eccessivi.

Articolo 5 - Responsabilità

L'utente è informato del fatto che la conoscenza delle credenziali di autenticazione da parte di terzi consentirebbe a questi ultimi l'utilizzo del sistema informativo e dei servizi erogati attraverso di esso; pertanto, è tenuto a non rivelare ad alcuno le proprie credenziali di autenticazione per l'accesso al sistema informativo.

L'utente è il solo ed unico responsabile della conservazione e della riservatezza delle proprie credenziali di autenticazione e, conseguentemente, rimane il solo ed unico responsabile per tutti gli usi ad essa connessi o correlati, (ivi compresi danni e conseguenze pregiudizievoli arrecati all'Ente e/o a terzi) siano dal medesimo utente autorizzati ovvero non autorizzati.

L'utente si impegna a comunicare immediatamente all'AdS l'eventuale furto, smarrimento o perdita della password. In particolare, in caso di furto, l'utente si impegna a modificare tempestivamente tale password utilizzando le procedure automatiche a sua disposizione.

Articolo 6 - Sanzioni

Qualsiasi utilizzo del S.I.C. non conforme alle disposizioni del presente regolamento e/o alle leggi vigenti è ad esclusiva responsabilità dell'utente.

Nei casi in cui si accertino violazione del regolamento, è demandata ai rispettivi Responsabili l'applicazione dei necessari provvedimenti disciplinari, fermo restando l'obbligo di segnalare al Titolare ed al Segretario Comunale ed alla competente autorità giudiziaria eventuali violazioni costituenti reato.

Allegato A - Modulo di presa visione e accettazione

Presenza visione ed accettazione del regolamento di utilizzo del Sistema Informatico Comunale

Il sottoscritto/a _____,
nato/a _____ il _____,
residente a _____ in via _____,
telefono _____ codice fiscale _____,
N° e tipo del documento di identità _____,

dichiara di:

- aver preso visione ed accettare tutte le norme contenute nel regolamento d'uso del Sistema Informatico del _____;

Data _____ Firma _____