



# COMUNE DI GALBIATE

## PROVINCIA DI LECCO

### REGOLAMENTO PER L'ACCESSO MEDIANTE VIRTUAL PRIVATE NETWORK (V.P.N.) AI SISTEMI INFORMATIVI DEL COMUNE DI GALBIATE

**Approvato con Deliberazione Giunta Comunale n. 83 del 29/04/2020**

#### INTRODUZIONE

Il Comune di Galbiate gestisce un sistema che consente ai dipendenti del Comune di accedere ai sistemi informativi dell'ente da postazioni esterne agli Uffici Comunali.

L'accesso a tali sistemi informativi è realizzato mediante un collegamento protetto su Rete Privata Virtuale (VPN, Virtual Private Network). L'accesso mediante collegamento VPN prevede la disponibilità di credenziali strettamente personali di tipo forte (tipicamente associate ad una Carta Nazionale dei Servizi) o di tipo debole (username e password).

Tale accesso è subordinato al rispetto del presente Regolamento, oltre che delle norme civili, penali e amministrative applicabili.

#### ART 1 - MODALITÀ DI ACCESSO INFORMATICO ALLA BANCA DATI DEL COMUNE DI GALBIATE

Il dipendente che intendesse utilizzare l'accesso ai dati informatici del Comune tramite collegamento VPN dovrà avanzare richiesta al Responsabile del Servizio Informatico e successivamente, avendone avuto titolo, previa ricezione delle necessarie credenziali per l'accesso VPN ai sistemi informativi del Comune di Galbiate, da parte dello stesso Responsabile, si impegna a rispettare il presente Regolamento.

In particolare si impegna a:

- 1) accedere esclusivamente ai servizi e ai sistemi informativi del Comune di Galbiate per i quali è stato espressamente autorizzato e con le modalità consentite;
- 2) assumere la personale responsabilità del mantenimento della necessaria riservatezza sulle proprie credenziali;
- 3) assumere la personale responsabilità delle attività svolte attraverso le credenziali a lui assegnate;
- 4) comunicare immediatamente al Segretario Comunale lo smarrimento, il furto o l'appropriazione da parte di terzi delle proprie credenziali;
- 5) segnalare immediatamente qualsiasi incidente o malfunzionamento;
- 6) non recar danno o pregiudizio ai software in dotazione agli Uffici Comunali o a terzi e a non interferire con l'utilizzo dei servizi di rete da parte di altri utenti;
- 7) rispettare le norme contenute nel presente Regolamento Accesso VPN e ad utilizzare le credenziali assegnate ai soli fini di fruizione dei servizi a cui è stato autorizzato.

In considerazione della struttura dell'Ente e delle difficoltà connesse all'assegnazione di un Personal Computer collegato con la rete comunale, i dipendenti sono autorizzati ad utilizzare per il collegamento i Personal computer personali a condizione che vengano garantite le misure minime di sicurezza (divieto di utilizzo chiavette USB, presenza di un antivirus installato).

## **AR. 2 - MODALITÀ DI UTILIZZAZIONE DELL'INFRASTRUTTURA INFORMATIVA A CUI SI ACCEDE**

È espressamente vietato utilizzare l'infrastruttura informatica a cui si accede per scopi incompatibili con quelli stabiliti nel presente Regolamento. In particolare, a titolo esemplificativo e non esaustivo, è vietato:

- 1) accedere all'infrastruttura informatica comunale per conseguire l'accesso a risorse di rete non autorizzate;
- 2) fornire il servizio di connettività di rete a soggetti non autorizzati all'accesso all'infrastruttura informatica comunale;
- 3) svolgere attività che causino malfunzionamento, diminuiscano la regolare operatività, danneggino o restringano l'utilizzabilità o le prestazioni dei sistemi di informatici comunali. E' altresì vietato impedire o interferire o tentare di impedire o interferire in qualsiasi forma con i servizi offerti tramite l'infrastruttura informatica comunale ad altri dipendenti;
- 4) violare la sicurezza di archivi e banche dati; compiere trasferimenti non autorizzati di informazioni (software, basi dati, ecc.); intercettare, tentare d'intercettare o accedere a dati in transito sull'infrastruttura informatica comunale, dei quali non si è destinatari specifici;
- 5) compiere azioni in violazione delle norme a tutela delle opere dell'ingegno, del diritto d'autore e del software;
- 6) distruggere o tentare di distruggere, danneggiare o tentare di danneggiare, intercettare o tentare di intercettare, accedere o tentare di accedere senza autorizzazione alla posta elettronica o ai dati di altri dipendenti o di terzi; usare, intercettare o diffondere o tentare di intercettare o diffondere password o codici d'accesso o chiavi crittografiche di altri dipendenti o di terzi, e in generale commettere o tentare di commettere attività che violino la riservatezza di altri Utenti o di terzi, così come tutelata dalle norme civili, penali e amministrative applicabili;
- 7) creare o diffondere immagini, dati o altro materiale potenzialmente offensivo, diffamatorio, o dal contenuto osceno. In particolare, è vietato la ricezione, la trasmissione o il possesso d'immagini pornografiche relative a minori;

## **ART. 3 - MONITORAGGIO**

Il Segretario Comunale effettuerà il monitoraggio e la misura delle attività di rete, originate dalle credenziali assegnate, al fine di garantirne funzionalità e affidabilità, nel rispetto del principio di pertinenza e non eccedenza, secondo quanto previsto dalla normativa vigente (D. Lgs. 196/2006 e SS.MM.II. e Regolamento UE 2016/679).

## **ART. 4 - VIOLAZIONI**

Il Comune di Galbiate nella persona del Segretario Comunale, adotta ogni misura necessaria per prevenire, reprimere e punire violazioni al presente Regolamento.

Chiunque abbia notizia di una violazione, avvenuta o temuta, al presente Regolamento, è tenuto a segnalarlo immediatamente al Segretario Comunale per i provvedimenti del caso.

Il Segretario Comunale può ordinare l'immediata cessazione dell'attività all'origine dell'abuso, adottando le necessarie misure per impedire ulteriori conseguenze ed individuare il responsabile.

In particolare, si riserva di sospendere e/o revocare le credenziali assegnate nel caso in cui venga rilevato un uso non corretto e comunque non conforme al presente Regolamento, notificando al dipendente ed al Sindaco le motivazioni di tale decisione. Accertata l'esistenza della violazione, il Segretario Comunale - sentito il dipendente comunale cui è imputata la violazione stessa - lo esclude temporaneamente o permanentemente, dall'accesso VPN.

Sono fatte salve le ulteriori conseguenze di natura penale, civile, amministrativa e disciplinare della violazione compiuta. In particolare, si rammenta che i comportamenti illeciti che integrano gli estremi di reati informatici ed elettronici, ai sensi della legge 48/2008 sono perseguibili dall'autorità giudiziaria e puniti a norma della legge penale.

## **ART. 5 - DISPOSIZIONI FINALI**

Per tutto quanto non espressamente contemplato dal presente Regolamento, valgono le disposizioni previste dalla normativa vigente in materia.

Il presente regolamento è da considerarsi a tutti gli effetti quale appendice del Regolamento Uffici e Servizi.

## **ART. 6 - ENTRATA IN VIGORE**

Il presente Regolamento entrerà in vigore ad avvenuta esecutività della relativa deliberazione di approvazione.