COMUNE DI VITTUONE
Città Metropolitana di Milano

REGOLAMENTO PER L'UTILIZZO DELLE RISORSE INFORMATICHE DEL COMUNE DI VITTUONE

Approvato con deliberazione della Giunta Comunale n. 36 in data 12/03/2026

Comune di Vittuone – Piazza Italia 5 – 20009 Vittuone (MI) tel: 02903201
Pec: ufficio.protocollo@pec.comune.vittuone.mi.it

Sommario

1. Principi generali

L'utilizzo delle risorse informatiche, telematiche e del patrimonio informativo del Comune di Vittuone deve sempre ispirarsi al principio della diligenza e della correttezza. Tali comportamenti devono sempre essere adottati dai dipendenti nell'ambito del rapporto di lavoro e da qualsiasi persona, a prescindere dal rapporto contrattuale intrattenuto con la stessa (collaboratori, consulenti, operatori esterni, amministratori...), venga autorizzata all'uso di tali risorse.

I due capisaldi sui si fondano le regole esposte nella presente policy informatica sono:

- è vietato ogni utilizzo di apparecchiature informatiche, di personal computer, delle reti e di dati, diversi dai fini strettamente istituzionali
- deve essere evitato qualsiasi comportamento che possa minare l'integrità del patrimonio informativo comunale e provocare danni al sistema informatico nel suo complesso

Di seguito si richiamano semplici regole di comportamento per evitare condotte che inconsapevolmente possono causare rischi alla sicurezza del sistema informatico e del patrimonio informativo.

2. Ambito di applicazione

Il Regolamento si applica ai seguenti soggetti di seguito complessivamente denominati "utenti" ovvero:

a) tutti i dipendenti, indipendentemente dalla modalità di svolgimento dell'attività lavorativa (solo a titolo d'esempio: telelavoro, smart working, ecc.);
b) i titolari di cariche politiche;
c) tutti coloro che svolgono attività per il Comune, quali: collaboratori e prestatori di lavoro autonomo a prescindere dal rapporto intrattenuto con l'amministrazione; in generale, a chiunque sia autorizzato all'utilizzo delle Dotazioni del Comune nello svolgimento delle proprie funzioni istituzionali.

3. Utilizzo del Personal Computer

1. Il Personal Computer affidato all'utente è uno strumento di lavoro ed è di proprietà esclusiva del Comune di Vittuone. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il personal computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento.

2. Il Personal Computer dato in affidamento all'utente permette l'accesso alla rete del Comune solo attraverso specifiche credenziali di autenticazione.

3. Il personale che opera presso il Servizio Informatico è autorizzato a compiere interventi nel sistema informatico comunale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware etc.). Detti interventi potranno anche comportare l'accesso in qualunque momento, ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché alla verifica sui siti internet acceduti dagli utenti abilitati alla navigazione esterna. La stessa facoltà,

sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Ente, si applica anche in caso di assenza prolungata od impedimento dell'utente.

4. Il personale incaricato del Servizio Informatico ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e di rete. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

5. Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale del Servizio Informatico né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre Virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone lo stesso Comune a gravi responsabilità civili; si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate anche penalmente e possono anche comportare il sorgere di una responsabilità amministrativa dell'Ente.

6. Salvo preventiva espressa autorizzazione del personale del Servizio Informatico, non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ...).

7.Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale del Servizio Informatico nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo articolo 8 del presente Regolamento relativo alle procedure di protezione antivirus.

8. Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. In ogni caso per assenze superiori ai 30 minuti è necessario bloccare lo schermo del PC proteggendolo con password. Lasciare un elaboratore 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.

4. Gestione e assegnazione delle credenziali di autenticazione

1. Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal personale del Servizio Informatico, previa formale richiesta del Responsabile del Settore nell'ambito del quale verrà inserito ed andrà ad operare il nuovo Utente.

2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dal Servizio Informatico, associato ad una parola chiave (password) riservata che dovrà venir custodita dall'incaricato con la massima diligenza e non divulgata.

3. La parola chiave, formata da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, deve essere composta da almeno otto caratteri, una lettera maiuscola e un numero e non deve contenere riferimenti agevolmente riconducibili all'incaricato.

4. È necessario procedere alla modifica della parola chiave a cura dell'utente, incaricato del trattamento, al primo utilizzo e, successivamente, almeno ogni sei mesi (Ogni tre mesi nel caso invece di trattamento di dati sensibili attraverso l'ausilio di strumenti elettronici).

5. Qualora la parola chiave dovesse venir sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, si procederà in tal senso d'intesa con il personale del Servizio Informatico.

6. Soggetto preposto alla custodia delle credenziali di autenticazione è l'incaricato dei Servizio Informatico del Comune.

5. Utilizzo della rete del Comune di Vittuone

1. Per l'accesso alla rete del Comune, ciascun utente deve utilizzare la propria credenziale di autenticazione.

2. L'account di accesso alla rete e relativa password, sono personali, non possono essere ceduti a terzi e devono essere custoditi in modo diligente; il titolare è pienamente responsabile di ogni suo uso od eventuale abuso.

3. È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato o con credenziali appartenenti ad un altro utente. La parola chiave d'ingresso alla rete ed ai programmi è segreta e va comunicata e gestita secondo le procedure impartite.

4. Le credenziali di autenticazione sono disattivate dal Servizio Informatico al termine del rapporto di lavoro o collaborazione con l'Ente. È compito del Responsabile del servizio personale, comunicare al Servizio Informatico quando un'utenza deve essere disattivata per le ragioni precedentemente esposte.

5. Le credenziali di autenticazione sono inoltre disattivate dopo tre mesi di inutilizzo da parte dell'utente a cui sono state assegnate;

6. La riattivazione delle credenziali è eseguita dal Servizio Informatico su richiesta dell'interessato, nei casi in cui esse siano associate a un dipendente in servizio che non ne abbia fatto uso per un periodo maggiore di tre mesi;

7. Le cartelle utenti/settori presenti nei server del Comune 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. Su queste unità vengono svolte regolari attività di manutenzione, controllo, amministrazione e back up da parte del personale del Servizio Informatico.

8. Tutti i dischi o altre unità di memorizzazione locali (es. disco C: interno PC) non sono soggette a salvataggio da parte del personale incaricato del Servizio Informatico. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente).

9. Il personale del Servizio Informatico può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.

10. Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

11. L'accesso alle risorse informatiche del Comune da parte di Ditte e/o Fornitori esterni viene concesso previa valutazione dei Rischi ed attraverso l'implementazione e l'uso di sistemi di controllo.

12. Nella gestione dei sistemi informativi dell'Ente il Servizio Informatico potrà acquisire informazioni generate dalle funzionalità insite nei sistemi stessi, quali ad esempio le informazioni sugli orari di accensione e spegnimento del Personal Computer, rilevati automaticamente tramite il sistema di autenticazione al dominio di rete e i log degli accessi a specifiche applicazioni o risorse di rete (file o cartelle), nonché circa l'aggiornamento dell'antivirus e installazione delle patch di sicurezza sulla singola postazione. Tali informazioni potranno essere utilizzate, ai sensi dei successivi punti, per tutti i fini connessi al rapporto di lavoro, sempre nell'ambito delle finalità individuate ai sensi del presente Regolamento e con espressa esclusione di qualsiasi forma di controllo sistematico e costante nei confronti degli Utenti dei sistemi stessi.

6. Utilizzo di altri dispositivi elettronici

1. Tutti i dispositivi elettronici forniti in dotazione al personale dell'ente sono da considerarsi strumenti di lavoro e in quanto tali sono di esclusiva proprietà dell'Ente. Non è quindi consentito l'utilizzo a carattere personale e non inerente all'attività lavorativa.

2. Sono annoverati tra questi i telefoni fissi dell'Ente, i PC portatili, i telefoni cellulari e gli smartphone, indipendente dalla possibilità degli stessi di accedere alla rete dell'Ente.

3. L'Utente è responsabile del singolo dispositivo assegnato e deve custodirlo con diligenza sia durate trasferte / spostamenti, sia durante l'utilizzo in ambiente di lavoro o in altri luoghi dove gli sia consentito effettuare la prestazione lavorativa. È necessario adottare ogni possibile cautela per evitare danni o sottrazioni. In questi casi l'Utente deve rivolgersi alla Propria Posizione organizzativa o ai riferimenti dell'Ente per la parte informatica o la telefonia.

4. Danni arrecati alle attrezzature o loro perdita dovuti ad incauta custodia saranno a carico dell'utente utilizzatore.

5. Il dispositivo non deve essere lasciato incustodito in zone a libero accesso, al fine di ridurre il rischio di furti. In caso di trasferte, il dispositivo non deve essere lasciato in macchina, nemmeno per brevi periodi, in parcheggi pubblici o comunque in zone non custodite.

6. Qualora tali dispositivi dovessero essere smarriti o rubati, l'affidatario deve immediatamente segnalare l'evento all'Amministratore di sistema, al fine di approntare le necessarie misure di mitigazione del danno.

7. Utilizzo e conservazione dei supporti rimovibili

1. Tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili nonché informazioni costituenti know-how dell'Ente, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

2. Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il personale del Servizio Informatico e seguire le istruzioni da questo impartite.

3. I supporti magnetici contenenti dati sensibili devono essere adeguatamente custoditi in armadi chiusi.

4. È vietato l'utilizzo di supporti rimovibili personali.

5. L'utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.

8. Utilizzo di PC portatili

1. L'utente è responsabile del PC portatile assegnatogli dal Servizio Informatico e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

2. Ai PC portatili si applicano le regole di utilizzo previste dal presente regolamento, oltre alle specifiche disposizioni contenute nell'informativa allegata all'accordo per lo svolgimento dell'attività lavorativa in modalità agile o da remoto

3. I PC portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

4. In caso di necessità di dismissione di un dispositivo, lo stesso dovrà essere preso in carico dai Sistemi Informativi che si occuperanno di effettuare una dismissione sicura dello strumento rendendo illeggibili i dati contenuti e dismettendolo nella maniera corretta.

5. Nel caso di riutilizzo di un dispositivo, i Sistemi Informativi effettueranno la cancellazione dei dati precedentemente presenti prima di metterlo a disposizione per il nuovo utilizzo.

9. Dispositivi BYOD (Bring Your Own Device – BYOD)

1. È possibile utilizzare dispositivi di proprietà (Bring Your Own Device - BYOD) per trattare dati dell'organizzazione solo se tale utilizzo è compatibile con le procedure di sicurezza previste nel contesto lavorativo e se preventivamente approvato dal rispettivo referente. Sul dispositivo dovranno essere applicate le medesime misure di sicurezza in uso per gli strumenti aziendali.

2. Per garantire l'utilizzo in sicurezza di tali strumenti potranno essere previste specifiche procedure e istruzioni per l'uso ad integrazione del presente disciplinare.

10. Utilizzo di piattaforme in cloud di file sharing

1. E' possibile utilizzare piattaforme di file sharing solo se facenti parte delle piattaforme consentite dai Sistemi Informativi o facenti parte della dotazione dell'organizzazione.

2. L'utilizzo di piattaforme alternative deve essere limitato allo stretto indispensabile ed autorizzato o da soggetti incaricati dall'organizzazione del coordinamento di tali aspetti.

11. Uso della Posta Elettronica

1. Il Servizio Informatico rende disponibile a Personale ed Amministratori dell'Ente, su richiesta del Responsabile di Settore, un indirizzo di posta elettronica istituzionale di regola denominata: nome.cognome@comune.vittuone.mi.it, da utilizzare per le comunicazioni ufficiali e istituzionali.

2. L'utilizzo degli indirizzi di cui al presente articolo costituisce "trattamento dei dati personali" e, pertanto, da conformarsi alle disposizioni del Regolamento UE 2016/679 e D.Lgs. 196/2003 e ss.mm.ii..

3. Il Personale e gli Amministratori dell'Ente possono accedere al servizio di posta elettronica utilizzando le credenziali a loro assegnate. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

4. Nel caso di assenza programmata, il dipendente è tenuto ad attivare sistemi di risposta automatica ai messaggi di posta elettronica ricevuti, nei quali indicherà eventuali indirizzi istituzionali alternativi ai quali fare riferimento per l'invio di comunicazioni.

5. Al fine di agevolare la comunicazione istituzionale e favorire la circolazione delle informazioni, sono altresì forniti indirizzi per unità/strutture organizzative o indirizzi legati alla carica, utilizzati prevalentemente per liste di distribuzione o caselle di posta elettronica, il cui accesso è consentito a uno o più lavoratori. A titolo esemplificativo, l'account di posta elettronica può essere fornito a:

a) Uffici, nella forma <acronimo ufficio>@<ente>.it;

b) Carica, nella forma <carica>@<ente>.it;

6. Il Servizio Informatico implementa misure di protezione automatizzate antivirus e antispam per il servizio di posta istituzionale, decidendone le tecnologie e le modalità operative, per contrastare la ricezione di messaggi di posta elettronica non desiderati contenenti virus, comunicazioni e/o materiali pubblicitari o altro materiale dal contenuto potenzialmente dannoso.

7. Il Servizio Informatico, pur adottando tutte le misure tecniche ritenute necessarie e sufficienti a minimizzare il rischio di perdita di informazioni di interesse dell'utente, non può essere ritenuto responsabile dell'eventuale cancellazione, danneggiamento, mancato invio, mancata ricezione o ritardo nella consegna di messaggi, se dovuti a malfunzionamenti o a guasti dei sistemi di posta, dei sistemi di protezione e di backup.

8. Il Servizio Informatico adotta le soluzioni tecniche che limitino la cancellazione immediata dei messaggi di posta identificati come spam, entro i limiti consentiti dall'infrastruttura adottata e salvaguardando, per quanto possibile, l'operatività degli utenti.

9. Il servizio di posta elettronica istituzionale sarà disattivato contestualmente il termine del rapporto con Ente.

10. La cancellazione di tutti i messaggi contenuti nella casella disabilitata avverrà dopo due mesi dalla disattivazione del servizio di posta elettronica.

11. Su richiesta motivata del relativo Responsabile di Settore, il Servizio Informatico può autorizzare l'accesso ad una Casella di posta istituzionale ad altri utenti dandone immediata informazione al diretto interessato, qualora assente per lunghi periodi.

12. La posta elettronica istituzionale è da considerarsi quale necessario strumento di lavoro e pertanto non deve essere utilizzata per scopi personali.

13. La posta elettronica, per via delle caratteristiche di sicurezza e tecnologiche intrinseche al servizio stesso, non è in alcun modo da considerare quale metodo di archiviazione di documenti. Deve essere considerata come canale di interscambio di corrispondenza e comunicazione e, pertanto, tutti i documenti allegati o comunicazioni contenenti informazioni personali o sensibili, devono essere scaricati e archiviati.

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

15. È obbligatorio porre la massima attenzione nell'aprire i file "attachements" di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

16. È vietato l'invio di messaggi di posta elettronica in nome e per conto di un altro utente, salvo sua espressa autorizzazione.

17. I messaggi di posta elettronica inviati non devono essere discriminatori o avere contenuti inappropriati che possano recare offesa al destinatario ovvero danno d'immagine all'Ente.

18. I dipendenti si uniformano alle modalità di firma dei messaggi di posta elettronica di servizio individuate dall'ente. Ciascun messaggio in uscita deve consentire l'identificazione del dipendente mittente e deve indicare un recapito istituzionale, anche telefonico, al quale il medesimo è reperibile.

12. Navigazione in Internet

1. Il PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento utilizzabile esclusivamente per lo svolgimento della propria attività. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.

2. In questo senso, a titolo puramente esemplificativo, l'utente NON potrà utilizzare internet per:

a. l'upload o il download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web, se non strettamente attinenti all'attività lavorativa (filmati e musica) e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà venir a tal fine contattato il personale del Servizio Informatico;
b. l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dal Responsabile del Settore;
c. ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;

d. la partecipazione a forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal Responsabile d'ufficio;

3. Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, il Comune di Vittuone è dotato di uno specifico sistema di blocco o filtro automatico per prevenire determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una black list.

4. Gli eventuali controlli, compiuti dal personale incaricato del Servizio Informatico, potranno avvenire mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta.

13. Protezione Antivirus

1. Il sistema informatico del Comune di Vittuone è protetto da software antivirus. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o mediante ogni altro software aggressivo.

2. È vietato disattivare il sistema antivirus presente sulla postazione, modificarne la configurazione o usare software antivirus differenti da quello fornito dall'Amministrazione.

Qualora si rilevino comportamenti anomali della propria postazione, deve essere tempestivamente informato il servizio informatico per assistenza tecnica.

14. Disposizioni in merito ai controlli

1. Il Comune, per motivi organizzativi o di sicurezza si riserva la facoltà di effettuare, attraverso i servizi informatici, controlli saltuari e occasionali, garantendo agli utenti il rispetto dei principi di liceità, pertinenza e non eccedenza previsti dalla Normativa Applicabile, da quanto previsto dai provvedimenti del Garante della Privacy, nonché il rispetto del divieto dei controlli a distanza dei lavoratori dipendenti.

2. Su richiesta dell'Autorità giudiziaria il Comune, tramite i servizi informatici, è tenuto ad effettuare qualsiasi controllo sull'utilizzo delle Dotazioni.

3. Il Comune si riserva, in particolare, di monitorare le reti e le Dotazioni nei seguenti casi:

a. necessità di effettuare verifiche sulla funzionalità e sulla sicurezza dei sistemi;
b. constatazione di utilizzo indebito della posta elettronica e della rete Internet;
c. necessità di effettuare verifiche tese alla protezione del patrimonio del Comune;
d. presenza di casi di abusi da parte di singoli o reiterati;
e. presenza di indizi relativi alla fuga di informazioni riservate o confidenziali.

4. Segnatamente, controlli periodici possono essere effettuati su: volume dei messaggi scambiati, formato e dimensione dei file allegati, durata dei collegamenti ad Internet (globale, per funzione, per gruppi o tipologia di utenti), siti visitati più frequentemente (globale, per funzione, per gruppi o tipologia di utenti), informazioni raccolte dai dispositivi di sicurezza (firewall, antivirus, IDS, IPS, ecc.).

5. Le informazioni relative ai file log vengono conservati per un periodo di 12 mesi e funzionalmente alla capienza dei server.

6. Le modalità con cui verranno effettuati i controlli saranno le seguenti:

a. i controlli, ove possibile, verranno effettuati preventivamente su informazioni appartenenti a gruppi collettivi di utenti, su dati aggregati e anonimi tramite l'analisi di statistiche generali;
b. successivamente, verranno inoltrati avvisi collettivi di diffida al compimento di operazioni non consentite o, a seconda della gravità, verranno prese misure di tipo individuale, specialmente in caso di abuso e/o anomalie reiterate
c. nei casi in cui si debba far fronte a particolari esigenze tecniche o di sicurezza oppure si debbano utilizzare i dati registrati con riferimento all'esercizio o alla difesa di un diritto in sede giudiziaria (azioni da parte di terzi verso il Comune o viceversa, o in caso di verifiche relative ad un presunto comportamento illecito), oppure si ottemperi all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria, tale periodo verrà prolungato secondo le necessità del caso e nel pieno rispetto delle finalità descritte;
d. in ogni caso verranno esclusi controlli prolungati, costanti o indiscriminati o comunque preordinati al controllo a distanza dei lavoratori. A tal riguardo si precisa che: in ogni caso non si fa luogo alla lettura e alla registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio email ivi inclusi i salvataggi periodici dei dati (c.d. "back up"); inoltre, non si procede alla riproduzione o memorizzazione sistematica delle pagine web visualizzate dall'utente, né alla lettura e alla registrazione dei caratteri inseriti tramite tastiera o analogo dispositivo.

7. L'Amministratore di Sistema può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericoloso per la sicurezza, sia sul PC degli utenti che sulle unità di rete.

8. L'effettuazione di tali controlli, che non hanno lo scopo di monitorare l'attività degli utenti, bensì di verificare la sicurezza del sistema e per effettuare la manutenzione, avverranno nel pieno rispetto della Normativa Applicabile.

9. Con il presente Regolamento è fornita informativa agli utenti, anche ai sensi dell'art. 13 del GDPR, in merito ai controlli e al relativo trattamento dati; l'eventuale conservazione di tali dati avverrà per il tempo strettamente limitato al perseguimento lecito di finalità.

15. Conservazione dei dati

1. Quotidianamente vengono salvati su sistemi esterni al data center tutti i dati relativi a: cartelle di rete, posta elettronica, file di Log. I supporti esterni, conservati per almeno 180 giorni, possono essere accessibili solo all'Amministratore di Sistema.

2. I file di Log contengono le informazioni relative ad almeno gli ultimi 180 giorni. I dati contenuti nei Log possono essere trattati in via eccezionale e tassativamente nelle seguenti ipotesi: per corrispondere ad eventuali richieste della polizia giudiziaria e/o dell'autorità giudiziaria, allorquando sia necessario un intervento – espressamente richiesto dall'utente – volto al recupero di dati contenuti in file o e-mail accidentalmente andati persi.

3. Il contenuto dei dispositivi di memorizzazione, delle cartelle dei file server, degli account di posta elettronica saranno conservati sul server centrale e/o sui backup del Comune per dieci anni, fatte salve eventuali esplicite richieste delle Autorità competenti e/o salvo che vi siano elementi che inducano il Comune stesso a ritenere necessario un periodo di conservazione più lungo (ad esempio, per finalità di giustizia), anche in seguito ad un'eventuale valutazione di impatto ai sensi e per gli effetti dell'art. 35 del GDPR.

4. Il traffico internet sarà cancellato dal Comune periodicamente, ogni dodici mesi, fatte salve eventuali esplicite richieste delle Autorità competenti e/o salvo che vi siano elementi che inducano il Comune stesso a ritenere necessario un periodo di conservazione più lungo (ad esempio, per finalità di giustizia), anche in seguito ad un'eventuale valutazione di impatto ai sensi e per gli effetti dell'art. 35 del GDPR.

16. Crittografia

1. L'utilizzo di sistemi di crittografia sulle risorse tramite cui vengono trattati dati di carattere professionale deve essere concordato con i Sistemi Informativi, al fine di garantirne la conformità alle politiche di crittografia definite a livello organizzativo.

2. Ogni attività di trasferimento verso l'interno e l'esterno dell'organizzazione di dati crittografati (sia tramite la connessione internet che tramite supporti fisici) dovrà essere concordata con i Sistemi Informativi.

3. L'organizzazione potrà effettuare verifiche sui sistemi e sulle attività di copia, scarico, trasmissione dati e custodia, per verificare l'eventuale presenza di dati crittografati non preventivamente concordati.

17. Sicurezza generale e perimetrale

1. All'interno dell'infrastruttura tecnologica è attivato un sistema di sicurezza perimetrale a difesa dei sistemi e dei dati, 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.

2. È gestito da soggetti debitamente designati dall'organizzazione, i quali effettuano attività di verifica delle segnalazioni attivate dal sistema stesso, con lo scopo di comprendere e prevenire eventuali minacce esterne.

3. Qualora il sistema attivato rilevi delle minacce a specifici indirizzi IP interni delle postazioni di lavoro, i Sistemi Informativi verificheranno le cause della minaccia rilevata insieme all'utente/utenti che abitualmente utilizza/utilizzano la postazione, con l'obiettivo di comprendere la natura dell'intrusione e prevenire eventuali danni.

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

18. Incidenti di sicurezza e Data Breach

1. Un qualsiasi incidente, occorso su dati informatici, cartacei o credenziali di accesso, può compromettere la sicurezza dei dati personali e in generale delle informazioni.

2. In caso di particolare gravità, l'incidente può comportare una vera e propria violazione, denominata data breach, che è obbligatorio notificare all'Autorità Garante per la protezione dei dati personali ai sensi dell'art. 33 del RGPD.

3. Si riporta di seguito un elenco, esemplificativo ma non esaustivo, di tipologie di data breach:
Distruzione (dati non più disponibili)
Perdita (dati non disponibili per il Titolare ma probabilmente in possesso di altri soggetti
Modifica (senza possibilità di ripristino)
Divulgazione non autorizzata
Accesso non autorizzato
Indisponibilità temporanea del dato

4. Qualora si riscontri un incidente di sicurezza sulle risorse messe a disposizione dall'organizzazione è necessario comunicarlo immediatamente al proprio superiore e contattare il Responsabile Protezione dati scrivendo a dpo@comune.vittuone.mi.it - documentando l'accaduto - al fine di approntare prontamente adeguate misure di mitigazione del danno. Eventuali procedure di gestione degli incidenti, generali o specificamente dedicate a particolari contenuti, saranno rese disponibili nella intranet dell'organizzazione.

19. Obbligo di rispetto del presente regolamento

1. Il rispetto del presente Regolamento è un obbligo per tutti coloro che utilizzano le risorse della Comune di Vittuone, in quanto rappresenta una garanzia di corretta gestione della sicurezza dei sistemi e dei dati personali.

2. Il mancato rispetto delle regole e delle misure di sicurezza elencate nel presente Regolamento implica la responsabilità personale dell'utente e costituisce una violazione, che potrà avere conseguenze di natura disciplinare o contrattuale – oltre che di potenziale rilevanza amministrativa o penale - in relazione e rapporto alla gravità del comportamento e dei potenziali rischi per il sistema e per i dati personali.

3. Nel caso in cui si riscontrino delle criticità che possano ledere la sicurezza del sistema informativo, il Comune di Vittuone potrà effettuare verifiche sull'utilizzo delle risorse strumentali concesse in dotazione agli utenti in conformità alle indicazioni riportate nel presente Regolamento. Qualora l'utilizzo delle risorse fornite in dotazione possa 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.

20. Osservanza delle regole relative alla normativa in tema di protezione dei dati personali e agli standard di sicurezza dell'organizzazione

1. Oltre a quanto indicato nel presente Regolamento è obbligatorio per ogni utente tenere comportamenti conformi alla normativa vigente in tema di protezione dei dati personali e relativa

regolamentazione in essere nel Comune di Vittuone. In particolare, gli utenti, nei contesti operativi di propria competenza, sono tenuti a fare quanto nelle loro possibilità per l'adozione di adeguate misure di sicurezza, ai sensi dell'art. 32 del GDPR.

2. Qualora, nell'ambito delle proprie attività lavorative, un soggetto riscontri che il trattamento di dati effettuato possa contravvenire alle prescrizioni del GDPR o del D. Lgs. 196/2003, è tenuto ad informarne tempestivamente il proprio Responsabile e il Servizio Informatico dell'Ente, al fine di concordare ed intraprendere i necessari interventi di adeguamento e eventuale mitigazione del rischio.

3. Ogni utente deve improntare le proprie attività al rispetto della massima riservatezza sulle informazioni di cui abbia conoscenza per motivi istituzionali o conoscenza incidentale. 5. L'impegno alla riservatezza dovrà essere osservato anche a seguito di modifica dell'incarico e/o cessazione del rapporto di lavoro.

Glossario

Internet	è la rete mondiale per la trasmissione dati che collega i server pubblici di società, enti pubblici, istituzioni, organizzazioni, soggetti privati.
Lan	Local Area Network, rete dati che interconnette le apparecchiature informatiche all'interno di un'organizzazione
Password	parola di sicurezza, è normalmente abbinata all'userid (utente) per formare le credenziali di autenticazione
Account	è quell'insieme di funzionalità, strumenti e contenuti attribuiti ad un utente ed è il meccanismo attraverso il quale il sistema informatico gli mette a disposizione un ambiente con contenuti e funzionalità (dati e programmi), isolandolo dalle altre utenze. Vi si accede attraverso le credenziali di autenticazione (riconoscimento) nome utente e password
Dominio	entità logica che individua un insieme di risorse comuni (file, cartelle, programmi), gestite da uno o più server, il cui accesso avviene mediante l'account
Virus informatico	programma informatico che all'insaputa dell'utente può compromettere in varia misura il pc, i programmi ed i dati su di esso ospitati
Backup	procedura di salvataggio dei dati e programmi su supporti magnetici a lunga durata ed alta capacità (tipicamente cassette a nastro)
Dischi di rete	supporti di memorizzazione di massa accessibili attraverso la rete dati e non fisicamente collocati sul pc dell'utente
Server	elaboratore dotato di particolari caratteristiche hardware (memoria, potenza del processore, affidabilità dei componenti, alimentazione) in grado di sopportare grossi carichi di lavoro e garantire continuità operativa
File server	server dedicato alla memorizzazione dei file degli utenti (dati e programmi) in modo centralizzato attraverso l'uso della rete dati
Proxy server	server dedicato a gestire e intermediare gli accessi ad Internet per conto dei pc residenti sulla lan comunale.
Log file	file di registrazione di eventi (es. accessi Internet) gestito da un server
Notebook	computer portatile (a volte chiamato anche "laptop")
Netbook	computer portatile caratterizzato da dimensioni e peso ridotti e maggiore portabilità
Chiavette USB	dispositivi portatili che vengono inseriti in apposite porte disponibili sui pc sia fissi che portatili, sono normalmente dispositivi di memorizzazione dati (in sostituzione degli ormai obsoleti floppy disk), ma possono anche essere dispositivi di collegamento a reti senza fili (wireless) quali Bluetooth e WiFi, e altro ancora
Webmail	modalità di accesso ad una casella di posta elettronica attraverso pagine web, mediante l'uso di un browser (Firefox, Internet Explorer, Opera, ecc…)
Black list	elenco di siti web il cui accesso è bloccato dal proxy server
White list	elenco dei soli siti web ammessi alla navigazione dal proxy server
Time-out	intervallo di tempo che definisce una scadenza di validità (di connessione, di password, ...)