Cremona
COMUNE DI CREMONA
Area Segretario Generale
Servizio ICT - Agenda digitale

POLICY PER L'UTILIZZO DEI SISTEMI INFORMATICI E TELEMATICI DEL COMUNE DI CREMONA

Indice

Indice generale
Premessa....4
Art. 1 - Oggetto e finalità....4
Art. 2 - Campo di applicazione....5
Art. 3 - Principi generali e di riservatezza nelle comunicazioni....5
Art. 4 – Gestione, assegnazione, revoca delle credenziali di accesso....7
Art. 5 – Postazioni di lavoro e altri dispositivi fisici....8
Art. 6 – Gli applicativi dell'Ente....10
Art. 7 – La rete dati dell'Ente....10
Art. 7.1 – Risorse Interne....11
Art. 7.2 – Le connessioni verso l'esterno – utilizzo di internet....12
Art. 8 – Utilizzo Posta elettronica....14
Art. 9 – Utilizzo telefoni, fax, stampanti-fotocopiatrici....17
Art. 10 – Utilizzo dei dispositivi rimovibili....18
Art. 11 – Referenti informatici....20
Art. 12 – Formazione trasversale....21
Art. 13 – Assistenza agli utenti e manutenzione....21
Art. 14 – Uso di dispositivi personali (BYOD)....22
Art. 15 – Smart Working e collegamenti alla rete interna da remoto....24
Art. 16 – Controlli sugli Strumenti....26
Art. 16.1 – Conservazione dei dati....28
Art. 17 - Sanzioni Disciplinari....28
Allegato A)....29

Registro delle modifiche

Versione	Data	Cambiamenti effettuati dall'ultima versione

Premessa

1. La presente Policy intende fornire a dipendenti, collaboratori e Amministratori del Comune di Cremona, denominati anche utenti, le indicazioni per una corretta e adeguata gestione delle informazioni, in particolare attraverso l'uso di sistemi, applicazioni e strumenti informatici dell'Ente.

2. Ogni utente è tenuto a rispettare questa Policy. La Policy è costituita da diversi articoli a seconda della tematica e per ogni articolo solitamente dà informazioni di tipo tecnico per poi definire le misure prescrittive.

3. Sono indicati come 'strumenti' i computer (Desktop, Notebook, ThinClient, Smarthphone, Tablet, Server, Printer, PenDrive,...), le risorse (Email, File Server, Software,...), la rete privata (Wired, Wifi), messi a disposizione dall'Ente; questi compongono il patrimonio informatico del Comune di Cremona. Rientrano nella definizione 'Strumenti' anche i computer personali quando usati per accedere alle risorse dell'Ente (vedi paragrafo dedicato allo *smart working*).

4. I dati personali e le altre informazioni dell'utente 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. Sono compresi i dati scambiati durante le attività di smart working.

5. Per tutela del patrimonio dell'Ente si intende la salvaguardia dei dati e delle informazioni trattati dal Comune di Cremona e la sicurezza informatica dei software e dei dispositivi informatici dell'Ente.

6. Le informazioni contenute nel presente documento sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro e/o alle collaborazioni, visto che la presente Policy 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 "General Data Protection Regulation".

Art. 1 - Oggetto e finalità

1. La presente Policy disciplina l'utilizzo degli strumenti per una corretta ed adeguata gestione delle informazioni aziendali alla luce di:
   a) 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";
   b) Regolamento Europeo 679/16 "General Data Protection Regulation" (d'ora in avanti Reg. 679/16 o GDPR) come recepito con dlgsl 101/2018 aggiornando il dlgsl 196/2003;
   c) "Linee guida del Garante per posta elettronica e internet" in Gazzetta Ufficiale n. 58 del 10 marzo 2007;
   d) articolo 23 del D.Lgs. n. 151/2015 (c.d. Jobs Act) che intervendo sulla legge n. 300/1970 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»;
   e) Normativa nazionale legge 2 maggio 2017, n. 81 e s.m.i., atti normativi dell'Ente;

f) Regolamento per la disciplina di nuove modalità spazio temporali di svolgimento della prestazione lavorativa (lavoro agile - smart working), approvato nel 2019 con delibera di Giunta comunale n. 106 quale Appendice al Regolamento sull'ordinamento generale degli uffici e dei servizi dell'Ente.

2. La finalità è quella di promuovere presso personale, collaboratori e Amministratori dell'Ente una corretta "cultura informatica" affinché l'utilizzo degli Strumenti sia conforme alle finalità dell'Ente e nel pieno rispetto della legge. Si forniscono a tutti gli utenti descritti nell'art.2 "Campo di applicazione" le indicazioni necessarie con l'obiettivo di elevare la sicurezza informatica e di evitare il verificarsi di qualsiasi abuso o uso non conforme.
3. La presente Policy è soggetta a revisioni e aggiornamenti periodici per riflettere le esigenze in continua evoluzione del Comune di Cremona e le tendenze tecnologiche emergenti. Si invitano tutti gli utenti a familiarizzare con questa Policy e a rispettarla nel corso delle loro attività lavorative.

Art. 2 - Campo di applicazione

1. La Policy si applica a tutti i dipendenti, senza distinzioni di ruolo e/o livello, a tutti i collaboratori dell'ente a prescindere dal rapporto contrattuale in essere, a operatori del Servizio Civile, Tirocinanti, nonché Amministratori, in quanto autorizzati ad accedere agli strumenti e alle risorse informatiche del Comune. Tali soggetti vengono indicati d'ora in avanti come "utenti".

2. Ogni utente è in possesso di specifiche credenziali di autenticazione. In ambito di trattamento dati l'utente può essere indicato anche come "autorizzato al trattamento".

3. Per meglio specificare, ai fini della presente Policy:
   - per "TITOLARE" si intende l'Ente Comune di Cremona cui competono le decisioni in ordine alle finalità e alle modalità del trattamento dei dati, ivi compreso il profilo della sicurezza;
   - per "STRUTTURA" si intende un'Area o un Settore o un Servizio o un Centro di Responsabilità del Comune di Cremona, diretto da un Dirigente;
   - per "AMMINISTRATORE DI SISTEMA" si intende il soggetto cui è conferito il compito di sovrintendere alle risorse del sistema informatico;
   - per "RESPONSABILE DEL TRATTAMENTO" si intende la persona fisica o giuridica, l'autorità pubblica, il servizio o l'organismo che tratta dati personali per conto del titolare del trattamento;
   - per "AUTORIZZATO AL TRATTAMENTO" si intende il soggetto che è stato autorizzato dal titolare o dal responsabile a compiere operazioni sui dati cui ha accesso.

Art. 3 - Principi generali e di riservatezza nelle comunicazioni

1. I principi a fondamento della presente Policy sono quelli espressi nel "Regolamento Generale sulla Protezione dei Dati" n. 679/2016 unitamente a quanto previsto dalla Linea guida del Garante per l'uso della posta elettronica e Internet -[doc. web n. 1387522] del 1 marzo 2007, dalla Linea guida in materia di trattamento di dati personali di

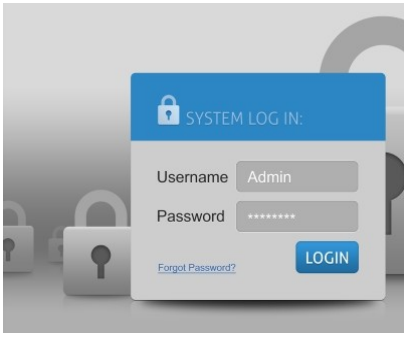
lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico -[doc. web n. 1417809] del 14 giugno 2007 e precisamente:

- il principio di **necessità**: i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione dei dati personali e di dati identificativi in relazione alle finalità perseguite;
- il principio di **correttezza**: le caratteristiche essenziali dei trattamenti devono essere rese note ai dipendenti. Le tecnologie dell'informazione consentono di svolgere trattamenti ulteriori rispetto a quelli ordinariamente connessi all'attività lavorativa all'insaputa o senza la piena consapevolezza dei dipendenti; l'Ente pertanto favorisce la formazione continua di tutto il personale e se possibile di tutti gli utenti, al fine di acquisire la necessaria consapevolezza nell'uso delle tecnologie informatiche e, più in generale, nel corretto utilizzo dei dati personali trattati per motivi di lavoro;
- principi di **pertinenza e non eccedenza**: i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime e nella misura meno invasiva possibile; le attività di monitoraggio effettuate sui sistemi informatici devono essere svolte solo da soggetti preposti ed essere mirate all'ambito oggetto di rischio per la rilevazione di eventuali e possibili data breach o per risolvere eventuali problematiche di tipo tecnologico.

2. Tutti gli utenti devono attenersi alle seguenti regole:

- è vietato comunicare a soggetti non specificamente autorizzati i dati personali comuni, le particolari categorie di dati (rif. art. 9 Reg.UE 679/16), i dati giudiziari e quelli sanitari o altri dati, elementi e informazioni istituzionali dei quali si viene a conoscenza nell'esercizio delle proprie mansioni all'interno del Comune. In caso di dubbio è necessario accertarsi che il soggetto cui devono essere comunicati i dati sia o meno autorizzato a riceverli mediante richiesta al responsabile del trattamento d'area;
- è vietata l'estrazione di originali e/o copie cartacee ed informatiche di documenti, fascicoli, lettere, data base, ecc. per uso personale;
- è vietato lasciare incustoditi documenti, fascicoli, ecc. che contengono dati personali e/o informazioni istituzionali quando ci si allontana dalla postazione di lavoro;
- è vietato lasciare sulla postazione di lavoro (scrivania, bancone ecc.) materiali che non siano inerenti la pratica che si sta trattando in quel momento. Ciò vale soprattutto nel caso di lavoratori con mansioni di front office;
- per le riunioni e gli incontri di particolare riservatezza dovranno essere utilizzate sale dedicate;
- l'attività di smart working deve essere svolta in ambienti che consentano il rispetto delle regole di cui sopra. In caso di problematiche di tipo informatico insorte nello svolgimento della prestazione lavorativa in modalità smart working, il dipendente è tenuto a darne pronta comunicazione al Servizio ICT e Agenda Digitale (d'ora in poi solo "Servizio ICT").

Art. 4 – Gestione, assegnazione, revoca delle credenziali di accesso



1. Le credenziali di autenticazioni (account) qui trattate riguardano gli accessi al dominio informatico dell'Ente e consistono in un codice per l'identificazione dell'utente (es. nome utente/password; nome utente/password/otp;…).
2. Tali credenziali vengono assegnate dall'Amministratore di Sistema o da un suo delegato del Servizio ICT direttamente all'utente, sono strettamente personali e l'utente è tenuto a conservarle nella massima segretezza, anche al di fuori del luogo di lavoro abituale.
3. La richiesta di nuove credenziali deve pervenire da referenti di settore abilitati; dirigenti, posizioni organizzative, referenti informatici, operatori locali di progetto (OLP).

   La richiesta di attivazione delle credenziali dovrà essere completa dei dati richiesti nelle forme predisposte dal Servizio ICT.

   È auspicabile che ogni utente fornisca un indirizzo email personale e/o un numero di telefono personale, così che il Servizio ICT lo utilizzi **esclusivamente** per la comunicazione di password (metodo più efficiente nel caso un utente non abbia ancora una casella di posta @comune.cremona.it o non possa accedervi per password dimenticata); in caso contrario verranno usate procedure alternative, adeguate a garantire che le credenziali siano a disposizione unicamente del titolare dell'account.
4. La password è personale e riservata e dovrà essere conservata e custodita dall'incaricato con la massima diligenza e non divulgata. Ad esempio non è contemplato scriverla su agende o post-it incustoditi, documenti word ecc.

   E' contemplato e consigliato l'utilizzo di Password Manager.
5. La password deve essere di adeguata robustezza.

   I sistemi di norma impongono questi requisiti minimi:

   - lunga almeno 8 caratteri
   - contenente almeno 3 dei seguenti tipi di carattere: lettere maiuscole, minuscole, numero, segno.

   Non deve contenere riferimenti agevolmente riconducibili all'utente (username, nomi o date relative alla persona o ad un famigliare) ed è preferibile che vada oltre i requisiti di cui sopra: una buona password è costituita da una breve frase, facile da ricordare, non famosa, meglio se strana, con qualche carattere come indicato.

   Il Servizio ICT ha in ogni caso facoltà di configurare i requisiti minimi e i parametri di validità, blocco e sblocco dell'account in funzione di quello che ritiene più opportuno per poter garantire al meglio la sicurezza dei sistemi.
6. È necessario procedere alla modifica della password a cura dell'utente al primo accesso e, successivamente, almeno ogni sei mesi. Nel caso in cui l'utente svolga mansioni che, in astratto, possano comportare il trattamento di categorie particolari di dati personali, può essere imposto il cambio password almeno ogni tre mesi.
7. E' assolutamente proibito entrare nella Rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato, ad esempio quello di un collega.
8. Nel caso di cessazione del rapporto di lavoro/collaborazione con l'utente, gli adetti alla gestione del rapporto di lavoro/collaborazione devono comunicare formalmente e preventivamente, all'Amministratore di Sistema e/o al Servizio ICT, la data effettiva di cessazione del rapporto.

9. L’amministratore di Sistema e/o il Servizio ICT ha facoltà di bloccare in qualsiasi momento un account qualora ne rilevi un uso illecito non rispondente alla presente Policy, o comunque potenzialmente dannoso per la sicurezza informatica dell’Ente.

Art. 5 – Postazioni di lavoro e altri dispositivi fisici

1. Gli strumenti informatici dell’Ente comprendono dispositivi fisici distribuiti in tutte le strutture dell’organizzazione. Tali dispositivi (PC Desktop, PC Notebook, Thin Client, Printer, Scanner ecc.) sono di proprietà del Comune di Cremona e possono, alla bisogna, essere utilizzati da qualsiasi operatore dell’Ente (in ottica di condivisione della strumentazione informatica) anche se solitamente usati da uno specifico utente (ad eccezione delle postazioni a rotazione).

2. I **Responsabili di Settori/Servizi** vigilano su l'implementazione e il mantenimento di questa Policy nei rispettivi ambiti organizzativi di competenza con riferimento circa: postazioni di lavoro, dispositivi fisici, sistemi e corretto utilizzo delle applicazioni utilizzate dalle postazioni di lavoro, rispetto delle procedure e accesso adeguato alla formazione sulla gestione delle informazioni e sulla sicurezza da parte del rispettivo personale. Nonché sull’adozione di procedure atte a garantire la non sottrazione e lo spostamento non concordato delle postazioni di lavoro e di altri dispositivi fisici.

3. In caso di furto o smarrimento di dispositivi fisici è obbligatoria sollecita denuncia alle autorità competenti. Inoltre è obbligatoria una pronta segnalazione ai canali di assistenza, in ogni caso entro 24 ore dall’evento, per una valutazione delle categorie dei dati contenuti nel dispositivo disperso. In caso di conferma o dubbio di presenza di dati personali sarà necessario far partire iter formali di denuncia nei confronti dell’Autorità Garante.
4. Allo scopo di gestire il parco dispositivi dell'Ente, ogni dispositivo fisico ha associata in inventario una collocazione fisica preferenziale. Qualsiasi spostamento permanente del dispositivo (es. trasloco, assegnazione ad altro reparto, assegnazione ad altro professionista) deve essere concordata con il Servizio ICT. La gestione ordinaria dei dispositivi fisici è in carico al Servizio ICT del Comune (e altri servizi coinvolti nella gestione dei beni informatici). È però demandata alla struttura che ospita i beni la gestione dei consumabili eventualmente presenti (es. toner delle stampanti, carta, etichette ecc.) attraverso coinvolgimento del Settore Economato.
5. Non è consentito l’utilizzo di dispositivi fisici informatici che non siano di proprietà del Comune o consentiti dallo stesso. Sistemi privati non consentiti non possono essere collegati alla rete dell'Ente.
6. Prescrizioni operative:

    1. Tutti gli strumenti informatici dell’Ente che siano acquisiti dal Servizio ICT o da altri Servizi/Settori devono essere inventariati e attivati dal Service Desk presso il Servizio ICT prima di essere utilizzati. Nessun dispositivo che non sia stato

preventivamente configurato e inventariato dal Service Desk può essere utilizzato dagli utenti dell'Ente.

2. L'utente è consapevole che gli Strumenti di proprietà del Comune di Cremona devono essere utilizzati esclusivamente per rendere la prestazione lavorativa. Ognuno è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione. Ogni utilizzo non inerente all'attività lavorativa è vietato in quanto può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.
3. PC Desktop, notebook, tablet, thin client ed ogni altro hardware devono essere custoditi con cura da parte degli assegnatari evitando ogni possibile forma di danneggiamento e segnalando tempestivamente al personale dell'Assistenza Informatica ogni malfunzionamento e/o guasto. E' vietato agli utenti modificare la configurazione hardware e software degli strumenti in dotazione senza preventiva autorizzazione da parte dell'Amministratore di Sistema.
4. Non è consentito all'utente modificare le caratteristiche hardware e software impostate sugli Strumenti assegnati, salvo preventiva autorizzazione da parte dell'Amministratore di Sistema.
5. L'utente è tenuto a scollegarsi dal sistema, o bloccare l'accesso (CTRL-ALT-CANC), ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro (PC) o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima: lasciare un PC incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.
6. Costituisce buona regola la pulizia periodica degli archivi memorizzati sul proprio PC e sulle cartelle del server, con cancellazione dei file obsoleti o non più utili.
7. È vietato utilizzare il PC per l'acquisizione, la duplicazione e/o la trasmissione illegale di opere protette da copyright.
8. È vietato connettere al PC qualsiasi periferica non autorizzata preventivamente dall'Amministratore di Sistema.
9. È assolutamente vietato connettere alla rete locale qualsiasi dispositivo (PC esterni, router, switch, modem, etc.) non autorizzato preventivamente dall'Amministratore di Sistema del Servizio ICT.
10. Nel caso in cui l'utente dovesse notare comportamenti anomali del PC, l'utente stesso è tenuto a comunicarlo tempestivamente all'Assistenza Informatica del Servizio ICT.
11. Salvo situazioni emergenziali, è necessario spegnere il personal computer al termine dell'attività lavorativa o in caso di assenza prolungata dal proprio ufficio, al fine di evitare l'accesso, anche fortuito, ai dati ivi contenuti, nonché per limitare il più possibile sprechi di corrente e rischi di incendio. Il PC dovrà essere bloccato ogni qualvolta rimanga incustodito anche per brevi periodi.
12. Il Servizio ICT del Comune di Cremona ha in gestione gli spostamenti e il magazzino delle postazioni di lavoro e dei dispositivi fisici. Lo spostamento di una postazione di lavoro o di un dispositivo fisico all'interno dello stesso settore deve essere autorizzato e richiesto dal Dirigente di Settore o dal Referente Informatico designato dal Dirigente, al Servizio ICT. Lo spostamento di una postazione di lavoro o di un dispositivo fisico tra settori diversi è gestito dal

Servizio ICT come dismissione di una postazione dal settore di provenienza, aggiornamento dell'asset e implementazione di nuova postazione nel settore di destinazione. I dirigenti dei Settori di provenienza e destinazione devono autorizzare e richiedere rispettivamente la disattivazione e l'attivazione attraverso i canali di ticketing predisposti.

Art. 6 – Gli applicativi dell'Ente

1. Il sistema informativo del Comune di Cremona comprende varie decine di applicativi aziendali, che possono essere di tipo web based, client server e stand alone. L'abilitazione agli applicativi aziendali (permessi di accesso e uso) è definita nel processo di gestione delle utenze.

2. Prescrizioni operative:

1. l'utente è consapevole che i software forniti, compresi quelli acceduti in modalità SaaS, sono di proprietà del Comune di Cremona e devono essere utilizzati esclusivamente per rendere la prestazione lavorativa. Ognuno è responsabile dell'utilizzo degli applicativi ricevuti in assegnazione. Ogni utilizzo non inerente all'attività lavorativa è vietato in quanto può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.
2. Non è consentito l'uso di applicativi non forniti dall'azienda, in quanto non è garantita la sicurezza degli stessi, e la rispondenza alla normativa vigente. Qualora emergesse l'esigenza di nuovi applicativi/soluzioni, gli operatori devono presentare, tramite il Dirigente della propria struttura, richiesta nella raccolta annuale del **Fabbisogno Informatico** (in occasione della costruzione del bilancio previsionale) o, in caso di esigenze sopravvenute e non rinviabili contattare il Servizio ICT per valutarne opportunità e modalità di adozione.
3. Non è consentito l'uso di applicativi aziendali per destinazioni diverse da quelle definite dall'organizzazione e dal fornitore del sistema.
4. Non è consentita l'installazione di programmi diversi da quelli autorizzati dall'Amministratore di Sistema.
5. Gli operatori del Servizio ICT, sentiti gli Amministratori di Sistema, monitorano periodicamente i software aziendali e possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la sicurezza dei PC, della rete locale e dei server dell'Ente, nonché rivedere/rimuovere tutte le impostazioni eventualmente configurate che possano interferire con il corretto funzionamento dei servizi informatici dell'Ente informandone i competenti responsabili.
6. È obbligatorio consentire l'installazione degli aggiornamenti di sistema e degli applicativi che vengono proposti automaticamente, al primo momento disponibile, in modo tale da mantenere il PC sempre protetto, fatte salve indicazioni diverse del Servizio ICT.

Art. 7 – La rete dati dell'Ente

1. La rete dell'Ente raggiunge oggi in modo capillare quasi ogni luogo fisico delle strutture comunali. E' composta da cablaggi fisici e rete WiFi.
2. Le performance della rete sono oggetto di continuo monitoraggio, in particolare nelle sedi centrali dell'Ente.
3. La connessione alla rete dell'Ente consente agli utenti di fruire di una serie di servizi, in particolare:

1. **Verifiche delle credenziali**: la rete consente agli operatori di accedere agli strumenti tecnologici dell'Ente solo se si è in possesso delle corrette credenziali.
2. **Accesso agli strumenti e alle risorse interne** quali ad esempio: Dischi di Rete, Intranet, applicativi aziendali, stampanti di rete, … In caso di indisponibilità della rete questi strumenti/risorse potrebbero risultare non raggiungibili.
3. **Accesso a internet:** la rete veicola l'accesso a internet per le postazioni di lavoro dell'Ente.

Art. 7.1 – Risorse Interne

Prescrizioni operative:

1. Gli strumenti di archiviazione messi a disposizione dall'Ente sono aree/spazi/cartelle di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi; pertanto qualunque file non riconducibile all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità; su queste vengono svolte regolari attività di controllo, amministrazione e backup da parte dell'Amministratore del Sistema.

2. Ogni Dirigente di Struttura è responsabile della definizione dei permessi di accesso alle risorse informatiche dedicati alla propria Struttura. Il Servizio ICT è a disposizione per attuare ruoli e permessi per conto del Dirigente se questi non risulta autonomo nell'operatività.
3. E' fortemente consigliato che i dati di interesse dell'Ente siano memorizzati sugli strumenti di archiviazione messi a disposizione dell'Ente, preferibilmente evitando l'esclusività dell'accesso (situazione problematica in caso di assenza del titolare).
   Gli strumenti di archiviazione messe a disposizione dall'Ente prevedono backup periodici mentre i dischi locali sui singoli PC, così come hard disk portatili, chiavette ecc., non danno garanzia di procedure analoghe di salvaguardia dei dati e pertanto il salvataggio esclusivo su questi dispositivi rende il titolare l'unico responsabile della custodia e dell'integrità dei dati stessi.
4. Senza il consenso dell'Amministratore di Sistema è vietato salvare documenti elettronici dell'Ente su repository esterni non approvati dal Comune (quali ad esempio Dropbox, GoogleDrive, OneDrive, ecc.).

5. Con frequenza periodica di almeno tre mesi, ciascun utente provvede 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.
6. Il personale addetto alla gestione della Rete può, in qualunque momento, procedere alla rimozione di ogni file che riterrà essere pericoloso per la Sicurezza informandone il competente referente.
7. I log relativi all'uso degli strumenti e delle risorse dell'Ente saranno registrati e potranno essere oggetto di controllo da parte del Titolare del trattamento, attraverso l'Amministratore di Sistema, per garantire la sicurezza informatica e la tutela del patrimonio dell'Ente. I controlli possono avvenire secondo le disposizioni previste nell'art. 16 della presente Policy.

   Le informazioni così raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto della presente Policy, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 679/16 "General Data Protection".

Art. 7.2 – Le connessioni verso l'esterno – utilizzo di internet

1. La rete dell'Ente consente l'accesso alla rete Internet dalla maggior parte delle postazioni di lavoro interne al Comune (potrebbero essere escluse postazioni che, per particolari requisiti di sicurezza e criticità, sono mantenute isolate).

2. L'accesso alla rete Internet è consentito nell'ambito dello svolgimento delle proprie attività professionali. Non è consentito l'uso a scopo personale. Per tale motivo l'azienda limita l'accesso alle risorse internet sulla base di sistemi di filtro automatico della navigazione verso dei siti web (es. sono esclusi siti classificati come pornografici, gioco online, trading online, ecc.) e della fruizione di specifici servizi (es. possono essere esclusi servizi di accesso ai social, streaming audio e video). Qualora alcuni siti web o alcuni servizi risultassero necessari per lo svolgimento dell'attività aziendale, e impropriamente resi non disponibili, è possibile contattare i servizi di assistenza facendo richiesta motivata e chiedendone l'abilitazione.

3. Il collegamento alla rete Internet è potenzialmente la sorgente principale di "infezione" della rete aziendale, intesa come lo scaricamento di dati e programmi (detti "malware") atti a minare l'integrità e la funzionalità della rete interna o sottrarre dati. Per tale motivo è importante che ogni operatore, che abbia accesso alla rete Internet, eviti di accedere a servizi non noti, o comunque estranei all'attività lavorativa e mantenga un atteggiamento cauto nell'utilizzo di servizi esterni alla rete aziendale. È obbligatorio inoltrare pronta segnalazione attraverso i canali di assistenza nel caso in cui, a seguito di navigazione sulla rete internet o utilizzo di servizi esterni alla rete aziendale, dovessero manifestarsi

comportamenti anomali della postazione di lavoro, o comunque qualora ci fosse il sospetto di tentativi di truffa/sottrazione dati/attacco informatico.

4. Prescrizioni operative:

    1. Durante le ore lavorative è ammessa solo la navigazione in siti considerati correlati con la prestazione lavorativa ad esempio i siti istituzionali, i siti degli Enti locali, di fornitori e partner dell'Ente. Gli accessi vengono registrati dal firewall dell'Ente.
    2. È vietato compiere azioni che siano potenzialmente in grado di arrecare danno all'Ente, 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.
    3. È vietato utilizzare programmi per la condivisione e lo scambio di file in modalità peer to peer o torrent ed è vietato scaricare file musicali, video e altro materiale non strettamente necessario per le attività lavorative.
    4. Durante le ore lavorative è vietata la partecipazione a Forum non professionali, ai Social Network, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).
    5. È vietato a chiunque il download di qualunque tipo di software gratuito (freeware) o shareware prelevato da siti Internet, se non espressamente autorizzato dagli Amministratori di Sistema.
    6. 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 l'Amministratore di Sistema per uno sblocco selettivo.
    7. 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, con il rispetto delle normali procedure di acquisto.
    8. È assolutamente vietato l'utilizzo di abbonamenti privati per effettuare la connessione a Internet tranne in casi del tutto eccezionali e previa autorizzazione degli Amministratori di Sistema.
    9. Per motivi tecnici e di buon funzionamento del sistema informatico è buona norma, salvo comprovata necessità, non accedere a risorse web che impegnino in modo rilevante banda, come a titolo esemplificativo: filmati (tratti da youtube, siti di informazione, siti di streaming ecc), in quanto possono limitare e/o compromettere l'uso della rete agli altri utenti.
    10. È vietato ascoltare la radio utilizzando le risorse Internet.
    11. L'accesso alla rete internet è monitorato, sia a tutela della sicurezza della rete dell'Ente, sia per prevenire eventuali usi impropri.
    12. 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, l'Ente registra per un periodo congruo (solitamente 180 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. Solo in casi eccezionali e di comprovata

urgenza rispetto alle finalità sopra descritte, l'Ente può trattare i dati di navigazione riferendoli specificatamente ad un singolo nome utente. In tali casi i controlli avverranno nelle forme indicate nell'art.16 della presente Policy. Le informazioni così raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto della presente Policy, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 679/16 "General Data Protection Regulation".

13. L'Amministratore di Sistema si riserva la facoltà di negare o interrompere l'accesso alla rete mediante dispositivi non adeguatamente protetti e/o aggiornati, che possano costituire una concreta minaccia per la sicurezza informatica dell'Ente.

Art. 8 – Utilizzo Posta elettronica

1. La posta elettronica può essere suddivisa in due tipologie: la posta elettronica ordinaria (PEO) e la posta elettronica certificata (PEC). La differenza tra le due è data dal fatto che con la PEC si ha la certezza, riconosciuta a livello legale, dell'invio e della consegna (o non consegna) del messaggio (come per la posta raccomandata).
2. I messaggi di posta elettronica ordinaria possono transitare su protocolli "in chiaro" (non criptati) anche se attualmente la tendenza dei servizi ICT è quella di configurare anche i server di posta ordinaria per la comunicazione su protocolli criptati. In ogni caso è fortemente sconsigliato utilizzare la posta elettronica ordinaria per trasmettere categorie particolari di dati personali.
3. La posta elettronica ordinaria può ulteriormente essere suddivisa in posta elettronica istituzionale e posta privata. La posta elettronica istituzionale è normalmente gestita dall'Ente a cui si appartiene ed è l'Ente che gestisce (anche come servizi) i server di posta e quindi è garante che i dati, in esso contenuti, non siano utilizzati per fini diversi da quelli istituzionali (il Comune di Cremona per esempio ha assegnato un mail server a cui fanno capo tutti gli indirizzi @comune.cremona.it).
4. Va ricordato che le caselle postali "gratuite" rese disponibili da varie aziende del mercato ICT (es. Google, Microsoft, ecc.) sono tali in quanto l'utente cede ai fornitori alcuni diritti di accesso e consultazione dei dati. Tali fornitori si riservano di utilizzare tali dati a scopo commerciale ivi compresa la possibilità di cedere parte delle informazioni a terze parti. La trasmissione di dati che si appoggi su tali servizi non è quindi riservata tra mittente e destinatario, ma coinvolge istituzionalmente il fornitore del servizio gratuito e l'ente non può in nessun modo farsi garante che i dati che transitano su queste caselle siano trattati secondo le attuali normative per il trattamento dei dati (GDPR). E' pertanto fatto divieto l'utilizzo di caselle private per fini istituzionali.
5. La Posta Elettronica Certificata (PEC), come precedentemente detto, garantisce la certezza dell'invio e del recapito (o del mancato recapito) e utilizza solo protocolli di comunicazione tra i server sicuri (il messaggio transita da una casella ad un'altra in maniera criptata); conseguentemente è uno strumento adeguato per la trasmissione di categorie particolari di dati personali.

6. Il Comune di Cremona predispone caselle PEC di gruppo per le strutture aziendali che, nell'ambito di convenzioni specifiche, necessitino di comunicare via PEC con istituzioni terze, professionisti e cittadini.
7. 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.

8. Prescrizioni operative:

    1. Ad ogni dipendente viene fornito un account e-mail nominativo, generalmente coerente con il modello nome.cognome@comune.cremona.it. Ai collaboratori, servizi civile, tirocinanti e altro personale non dipendente, viene fornito un account email generalmente coerente con il modello nome.cognome@ext.comune.cremona.it.

        L'utente a cui è assegnata una casella di posta elettronica è responsabile del corretto utilizzo della stessa. Il servizio ICT stabilisce i criteri di robustezza e blocco della password. È necessario procedere alla modifica della password, a cura dell'utente, al primo accesso e, successivamente ogni 3 mesi o con tempistiche diverse definite dal Servizio ICT. E' facoltà dell'Amministratore del sistema porre delle restrizione del periodo di validità della password in caso si reputi necessario innalzare i livelli di sicurezza.
    2. L'Ente fornisce, su richiesta, degli indirizzi di posta elettronica associati a ciascuna unità organizzativa, uffici o gruppi di lavoro il cui utilizzo è da preferire rispetto alle e-mail nominative qualora le comunicazioni siano di interesse collettivo, ed in particolare negli scambi con l'esterno.
    3. La casella di posta elettronica istituzionale assegnata dal Servizio ICT del Comune di Cremona deve essere gestita con l'interfaccia web. Non possono essere usati client locali di posta (es. Thunderbird, Ms Mail, Outlook ecc.), se non espressamente autorizzati e configurati dal Servizio ICT.
    4. La casella di posta istituzionale non può essere configurata per reindirizzare messaggi verso altri sistemi di posta esterni e viceversa: non si prevedono quindi inoltri automatici verso caselle di posta esterne, diverse da ..@comune.cremona.it. In via eccezionale gli inoltri automatici potranno essere attivati verso gestori di posta esterni ma già nominati responsabili per il trattamento dati dell'Ente e comunque dovranno essere espressamente autorizzati dal Servizio ICT.
    5. La trasmissione/ricezione delle comunicazioni tramite l'account di posta elettronica assegnata è consentita solo per scopi legati all'attività del Comune di Cremona. E' vivamente sconsigliato l'uso della posta elettronica per i contatti interpersonali tra lavoratori non inerenti la normale attività d'ufficio; in nessun caso l'indirizzo di posta elettronica istituzionale può essere utilizzato come proprio recapito e-mail "personale" per attività non inerenti quella lavorativa.
    6. Il Comune di Cremona, in caso di sospette violazioni, può verificare il traffico di posta, per il tramite dell'Amministratore di Sistema, secondo le modalità conformi alla normativa vigente e alle disposizioni del Garante per la Protezione dei Dati Personali, nel rispetto dei principi generali di trasparenza, liceità, correttezza, integrità e riservatezza.
    7. In caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, 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 titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.

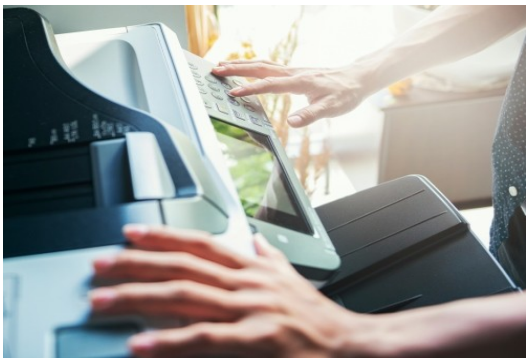
8. In caso di cessazione del rapporto lavorativo, il Servizio ICT procederà al blocco dell'account di posta del soggetto in uscita il giorno successivo alla cessazione. La casella di posta non sarà accessibile, ma continuerà ad essere un indirizzo attivo per 30 giorni; con adeguato anticipo sulla cessazione il titolare dovrà provvedere ad impostare avviso automatico relativo alla chiusura della casella, indicando il nuovo indirizzo a cui inviare le email (l'auto-responder è l'unico modo per dare contezza al mittente che la sua mail non è stata e non verrà letta).
   Successivamente la casella verrà chiusa completamente e cesserà di ricevere posta. Dopo ulteriori 30 giorni la casella verrà cancellata eliminando l'intero contenuto.
   Analogamente a quanto previsto per i dati, il dipendente prossimo alla cessazione, ha l'obbligo di trasmettere le email essenziali alla sua struttura di riferimento.
9. La posta elettronica non deve essere usata in modo da arrecare danno al Comune di Cremona o a terzi. In particolare va prestata attenzione ai messaggi e-mail i cui contenuti o mittenti appaiano sospetti o improbabili e ai messaggi contenenti link che rimandano a pagine richiedenti conferma o rinnovo delle credenziali interne all'ente (di dominio o di posta). Tali messaggi potrebbero potenzialmente veicolare spam, virus informatici, truffe o phishing; questi messaggi devono essere cancellati dalla casella di posta (preferibilmente usando la marcatura "spam" presente nella schermata iniziale di Zimbra e cancellandoli dalla posta indesiderata), senza effettuarne l'apertura; qualora inconsapevolmente non venga osservata questa norma, il dipendente deve avvisare tempestivamente il Servizio ICT; fermo restando che, se venisse riscontrata una precisa volontà del dipendente al non rispetto di tale indicazione, la responsabilità di eventuali danni è del dipendente.
10. Non è 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 vietato l'invio di messaggi pubblicitari di prodotti di qualsiasi tipo.
11. Nel caso fosse necessario inviare allegati "pesanti" (fino al 10 MB) è opportuno ricorrere prima alla compressione dei file originali in un archivio di formato .zip o equivalenti. Nel caso di allegati ancora più voluminosi è necessario rivolgersi all'Amministratore di Sistema.
12. Nel caso in cui fosse necessario inviare a destinatari esterni messaggi contenenti allegati con categorie particolari di dati personali, questo va fatto soltanto a destinatari - persone o Enti – qualificati e competenti. E' importante verificare che il destinatario sia in possesso dei titoli che lo abilitano al trattamento di quei particolari dati. Questa tipologia di dati va sempre trasmessa in maniera criptata.
13. La diffusione massiva di messaggi di posta elettronica deve essere effettuata esclusivamente per motivi inerenti il servizio. 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.
14. È vietato inviare posta elettronica in nome e per conto di un altro utente, salvo sua espressa autorizzazione.
15. La casella di posta elettronica, personale e quella relativa al gruppo ufficio, 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 unità di rete condivise.
16. I messaggi in entrata vengono sistematicamente analizzati alla ricerca di virus e malware e per l'eliminazione dello spam. I messaggi che dovessero contenere virus

vengono eliminati dal sistema. Altri messaggi considerati sospetti vengono messi nella cartella Spam (i messaggi contenuti nello Spam dovrebbero essere di norma non aperti ed eliminati a meno che non si abbia l'assoluta certezza della loro provenienza e della loro bontà). L'utente deve porre molta attenzione perché la mail sbloccata può contenere virus, malware, sistemi di phishing.

Articoli sulla intranet (sicurezza informatica), supporto dei referenti informatici e del Servizio ICT sono a disposizione per una consapevolezza maggiore.

17. L'Ente, per il tramite dell'Amministratore di Sistema, non controlla sistematicamente 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. Tuttavia, in caso di assenza improvvisa o prolungata del dipendente ovvero per imprescindibili esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'ente ovvero per motivi di sicurezza del sistema informatico, l'ente per il tramite dell'Amministratore di Sistema può, seguendo i principi del Regolamento europeo UE 2016/679, e delle misure minime di sicurezza Agid (circolare 2/2017) accedere all'account di posta elettronica, prendendo visione dei messaggi, salvando o cancellando file.

Art. 9 – Utilizzo telefoni, fax, stampanti-fotocopiatrici



1. Il telefono affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, e quindi non sono consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa.
2. La ricezione o l'effettuazione di telefonate personali sono consentite solo nel caso di comprovata necessità ed urgenza.
3. Se assegnato, l'utente è responsabile dell'utilizzo e della custodia dello smartphone istituzionale. E' vietata l'installazione e l'utilizzo di applicazioni diverse da quelle autorizzate dall'Amministratore del Sistema.
4. Agli smartphone dell'Ente (di servizio) si applicano le medesime regole previste per gli altri dispositivi informatici per quanto riguarda il mantenimento di un adeguato livello di sicurezza informatica e la corretta navigazione in internet.
5. È deprecato l'utilizzo dei fax.
6. È vietato l'utilizzo delle fotocopiatrici e delle stampanti per fini personali, salva diversa esplicita autorizzazione da parte del responsabile dell'area.
7. Per quanto riguarda l'uso delle stampanti gli utenti sono tenuti a:
    1) stampare i documenti solo se strettamente necessari allo svolgimento della propria attività; evitare la stampa di documenti o file molto lunghi in modo da evitare inutili sprechi;
    2) utilizzare preferibilmente le stampanti di rete condivise rispetto a quelle locali/personali, per ridurre il consumo di materiali (toner, ecc.);
    3) stampare in bianco/nero e fronte/retro per ridurre i costi.
8. Nel caso di stampa di informazioni riservate, l'utente dovrà presidiare il dispositivo di stampa per evitare la possibile perdita o divulgazione di tali informazioni a persone

terze non autorizzate o utilizzare il codice di stampa personale sulla stampante per permettere l'effettiva stampa.

Art. 10 – Utilizzo dei dispositivi rimovibili

1. La presente Policy è stata sviluppata per garantire la sicurezza dei dati e delle informazioni del Comune di Cremona nell'uso di dispositivi rimovibili. L'obiettivo è minimizzare il rischio di perdita di dati, furto, o compromissione dei sistemi informatici.
2. L'uso non controllato di dispositivi rimovibili può portare a perdite finanziarie significative, furto di informazioni, introduzione di malware e perdita di reputazione.
3. Pertanto, i dispositivi rimovibili dovrebbero essere utilizzati come ultima risorsa per memorizzare o trasferire informazioni.
   Normalmente, le informazioni dovrebbero essere memorizzate su sistemi aziendali e scambiate attraverso connessioni protette e approvate.
4. I "dispositivi rimovibili" si riferiscono a qualsiasi dispositivo di archiviazione dati che può essere facilmente rimosso da un sistema informatico e che è utilizzato per trasportare e trasferire dati da un sistema all'altro. Questi dispositivi includono, ma non sono limitati a:
   - Dischi rigidi esterni
   - Chiavette USB (anche note come pen drive o flash drive)
   - Schede SD
   - Dispositivi mobili
   - Lettori di schede di memoria
   - Microchip incorporati (inclusi smart card e SIM card di telefoni cellulari)
   - Lettori MP3
   - Fotocamere digitali
   - Cassette di backup
   - CD
   - DVD
   - Dischi ottici
5. È importante notare che questa definizione è intesa per essere inclusiva e non esclusiva. Pertanto, qualsiasi dispositivo che non è specificamente elencato ma che ha la capacità di memorizzare o trasferire dati è considerato un dispositivo rimovibile ai fini di questa Policy.
6. L'uso accettabile dei dispositivi rimovibili deve essere guidato dai seguenti principi:
   1. I dispositivi rimovibili devono essere utilizzati solo quando strettamente necessario. Normalmente, le informazioni dovrebbero essere memorizzate su sistemi aziendali e scambiate attraverso connessioni protette e approvate.
   2. I dispositivi rimovibili devono essere protetti da software antivirus e antimalware quando collegati a una macchina.
   3. Solo i dati autorizzati e necessari per il trasferimento dovrebbero essere salvati sui dispositivi rimovibili. Si ricorda che i dati eliminati possono ancora essere recuperati.

4. I dispositivi rimovibili non devono essere utilizzati per l'archiviazione o la conservazione di record come alternativa ad altre attrezzature di archiviazione.
5. È necessario prestare particolare attenzione alla protezione fisica del dispositivo rimovibile e dei dati memorizzati da perdita, furto o danni. Chiunque utilizzi dispositivi rimovibili per trasferire dati deve considerare il modo più appropriato per trasportare il dispositivo e essere in grado di dimostrare che ha preso le dovute precauzioni per evitare danni o perdite.
6. Per consigli o assistenza su come utilizzare in modo sicuro i dispositivi rimovibili, si prega di contattare il Servizio ICT.

7. Protezione dei Dati

   La protezione dei dati è di fondamentale importanza per garantire la sicurezza delle informazioni e la conformità con il GDPR.
   Le seguenti misure devono essere adottate per proteggere i dati sui dispositivi rimovibili:

   - **Crittografia**: I dati sensibili o personali su dispositivi rimovibili devono essere crittografati secondo gli standard riconosciuti. Questo garantisce che i dati siano inaccessibili senza la chiave di crittografia corretta.
   - **Password**: I dispositivi rimovibili devono essere protetti con password robuste. Questo fornisce un ulteriore livello di sicurezza, impedendo l'accesso non autorizzato ai dati.
   - **Software Antivirus**: Prima di trasferire dati su un dispositivo rimovibile, sia il dispositivo che il sistema da cui provengono i dati devono essere sottoposti a una scansione con software antivirus e antimalware approvati.
   - **Eliminazione sicura dei dati**: Quando un dispositivo rimovibile non è più necessario o deve essere riutilizzato, tutti i dati devono essere eliminati in modo sicuro. Questo deve essere un'eliminazione completa di tutti i dati dal dispositivo, utilizzando software e strumenti specializzati.
   - **Aggiornamenti del Software/Firmware**: Per garantire la massima sicurezza, i dispositivi rimovibili, ove possibile, devono essere sempre aggiornati con l'ultimo software/firmware. Questo aiuta a proteggere contro le vulnerabilità note che potrebbero essere sfruttate dagli attaccanti.
   - **Responsabilità dell'utente**: Gli utenti devono aderire a tutte le considerazioni di questa Policy quando utilizzano dispositivi rimovibili. Devono prestare particolare attenzione alla protezione dei dati quando utilizzano dispositivi come chiavette USB, hard disk esterni, CD registrabili, DVD e dischi.

8. L'utilizzo dei supporti di memoria removibili NON è consentito, tranne nei casi strettamente necessari ove non vi siano alternative.
9. Qualsiasi dispositivo rimovibile utilizzato in connessione con l'attrezzatura o la rete del Comune di Cremona o per detenere informazioni utilizzate per attività dell'Ente, in uso ai settori, deve essere acquistato e installato dal Servizio ICT o con approvazione di specifiche tecniche da parte del servizio ICT. Gli utenti non devono utilizzare alcun dispositivo rimovibile che non sia stato fornito o approvato dal Servizio ICT.
10. In caso di utilizzo, i supporti di memoria rimovibili contenenti categorie particolari di dati personali, nonché informazioni costituenti know-how, 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. In ogni caso, tali supporti devono essere adeguatamente custoditi in armadi chiusi e in caso di alienazione devono essere distrutti o formattati.

11. L’utente è responsabile della custodia dei supporti di memorizzazione e dei dati in essi contenuti.
12. È vietato l’utilizzo di supporti rimovibili personali sulla rete ed apparecchiature di lavoro.
13. Tutti i supporti USB (di memoria) prima di essere utilizzati all’interno del sistema, devono essere necessariamente validati dall’Amministratore di Sistema e devono essere soggetti a scansione e criptazione in caso di esportazione di dati. Non è consentito infatti l'utilizzo, non autorizzato, di supporti magnetici di provenienza ignota (chiavette USB, hard disk esterni, CD-ROM, DVD, ecc.).
14. Non è consentito scaricare nella Rete dell’Ente file contenuti in supporti magnetici/ottici non aventi alcuna attinenza con la propria prestazione lavorativa.
15. E' da evitare la copia su supporti portatili di memorizzazione di categorie particolari di dati personali - ex sensibili (art. 9 del Reg. UE 679/16) e/o dati personali per ridurre al minimo il rischio di perdita o distruzione anche accidentale dei dati stessi ovvero il cosiddetto data breach.
16. Qualora il contenuto del supporto di memorizzazione (o memoria USB) debba essere copiato su un hard disk locale od altro strumento elettronico di trattamento, è necessario accertarsi di cancellare il relativo contenuto al termine dell'operazione di trattamento.
17. Prestare particolare attenzione affinché nessun dato rimanga nella memoria buffer, nella clipboard, negli appunti o all'interno del cestino, qualora si faccia uso di dispositivi mobili su sistemi operativi di tipo Windows.
18. I supporti DVD, CD-ROM, USB, hard disk ecc., qualora contengano dati personali, devono essere trattati (protetti o cifrati) per evitare l’eventuale recupero dei dati da parte di soggetti non autorizzati. In particolare, se contenenti particolari categorie di dati, devono essere custoditi in contenitori ovvero in archivi chiusi a chiave.
19. È altresì opportuno:
    - evitare di lasciare incustoditi i supporti di memorizzazione, anche per breve periodo, poiché gli stessi possono essere rapidamente letti e copiati;
    - identificare ogni supporto di memorizzazione, per evitare di confonderli e generare un possibile data breach;
    - proteggere con apposite buste o contenitori, che ne dimostrino l’effrazione, i supporti di memorizzazione spediti o consegnati a terzi;
    - in caso di alienazione:
        - per CD e DVD provvedere alla distruzione rigando la superficie per poi spezzarli;
        - per memorie USB e hard disk provvedere alla formattazione a basso livello (ossia formattazione completa che garantisce la cancellazione definitiva dei dati).

Art. 11 – Referenti informatici

1. Il Servizio ICT si è organizzato individuando, al proprio interno, una persona di riferimento per ogni Settore dell'Ente per quanto riguarda gli applicativi in uso e i progetti con riferimenti informatici che il settore intende mettere in campo. Si tratta di Referenti ICT per Applicativi Progetti a cui i settori devono riferirsi quando intendono

adeguare/evolvere gli applicativi usati al loro interno e quando si prospetta un nuovo progetto che abbia necessità di strumenti informatici o che possa avere attinenza con strumenti informatici in uso presso altri settori.

2. Inoltre ogni settore, tenendo in considerazione un'eventuale proposta del Servizio ICT, dovrà nominare Referenti Informatici di Settore che siano in grado di contribuire all'innovazione tecnologica e alla digitalizzazione che l'Ente ha predisposto e sta sviluppando. Si tratta di persone che hanno una certa formazione e una certa predisposizione tecnologica in grado di elevare il livello culturale informatico del settore e di poter fare da tramite, se necessario, con il Servizio ICT. L'Ente potrà prevedere una specifica formazione aggiuntiva e aggiornata per i referenti informatici, la cui programmazione sarà inclusa nel Piano Formativo dell'anno di riferimento.
3. Al Referente sarà assegnato il compito di:
    - collaborare con il dirigente per segnalare al Servizio ICT il Fabbisogno Informatico annuale per la costruzione del Bilancio Previsionale;
    - collaborare con il Servizio ICT nella supervisione sul corretto utilizzo delle risorse informatiche;
    - predisporre e mantenere le cartelle di rete della propria struttura come indicato nell'art. 7.1 comma 1;
    - dare supporto nelle progettualità per tutto ciò che riguarda l'ambito informatico, oltre che fornire la propria collaborazione ai referenti della formazione negli ambiti di cooperazione trasversale;
    - dare supporto ai colleghi del settore nel livello operativo informatico (sia nell'uso degli applicativi sia nell'informatica di base) per competenze specifiche non previste dalla formazione somministrata dall'Ente (da concordare con dirigenti/amministrazione);
    - dare supporto agli operatori ICT nel formulare le esigenze tecniche del proprio Settore e nel sostenere saltuariamente piccoli interventi massivi sulle macchine degli utenti;
    - collaborare con il Referente ICT per Applicativi Progetti.

Art. 12 – Formazione trasversale

1. Tra le aree formative interessate dal Piano Formativo dell'Ente vi è l'Area informatica: essa comprende la formazione specifica su applicativi gestionali specifici e generali (videoscrittura, fogli di calcolo, ecc.) di uso comune, nonché l'aggiornamento del personale tecnico dell'ICT in conseguenza di innovazioni organizzative e dell'evoluzione tecnologica. Si vuole confermare anche una nuova modalità formativa (oltre a quella d'aula e a quella e-learning): quella erogata attraverso i video, nella considerazione del suo impatto più semplice e diretto. In tale quadro organizzativo si collocano gli interventi trasversali avviati e di futura implementazione e potenziamento dedicati alla formazione sulla Sicurezza informatica (Cybersecurity) e alle competenze digitali.

2. L'Ufficio Formazione si coordinerà con il Servizio ICT per individuare interventi di interesse strategico.

Art. 13 – Assistenza agli utenti e manutenzione

1. Qualora gli utenti riscontrino problemi informatici di qualsiasi tipo, possono inoltrare una richiesta di assistenza al personale interno tramite ticket dal sito intranet http://www.cr.comune, *accedi a, assistenza informatica* (e se richiesto digitare le credenziali della Intranet), descrivendo il problema e fornendo sempre uno screenshot di eventuali messaggi d'errore.
2. Non solo in caso di problemi ma anche in caso di richieste (mobilità/trasloco, nuovo hardware, nuovo software) è essenziale aprire un ticket tramite la stessa piattaforma.
3. Le richieste di assistenza informatica pervenute con specifica piattaforma di ticketing vengono tracciate e gestite; permettono l'immediata assegnazione al tecnico competente, la tracciabilità degli interventi effettuati, il riscontro della risoluzione della chiamata. Per tanto tali richieste sono prioritarie rispetto a richieste effettuate con altri canali (telefonate, email).
4. Qualora l'utente interno non riesca ad effettuare un ticket (ad esempio in caso di postazione di lavoro bloccata) può avvalersi del supporto del Referente informatico del proprio Settore per inoltrare la richiesta.
5. L'operatore di Service Desk, in base alla tipologia dell'intervento richiesto, può accedere ai dispositivi informatici comunali sia direttamente, sia mediante software di accesso remoto, per:
   - verifica e risoluzione di problemi sistemistici ed applicativi, su segnalazione dell'utente;
   - verifica del corretto funzionamento dei singoli dispositivi in caso di problemi rilevati nella rete;
   - richieste di aggiornamento software e manutenzione preventiva hardware e software.
6. Quando l'intervento richiede l'accesso ad aree personali, è necessario il consenso dell'utente. Qualora l'intervento tecnico in loco o in remoto non necessiti di accedere mediante le credenziali dell'utente, l'Amministratore del Sistema è autorizzato ad effettuarlo senza il consenso dell'utente cui la risorsa è assegnata.
7. L'assistenza da remoto sui PC della rete comunale da parte di terzi (fornitori) deve essere sempre preventivamente concordata con l'Amministratore di Sistema. Sarà l'Amministratore di Sistema che insieme al **Comitato di Sicurezza** stabilirà le tecnologie e le modalità operative che potranno essere utilizzate. Durante questi interventi l'utente richiedente o l'Amministratore di Sistema devono presenziare in modo da verificare ed impedire eventuali comportamenti non conformi alla presente Policy.

Art. 14 – Uso di dispositivi personali (BYOD)

1. La presente Policy definisce le linee guida per l'uso dei dispositivi personali nell'ambito delle attività lavorative presso il Comune di Cremona. Il concetto di "Bring Your Own Device" (BYOD) si riferisce all'uso di dispositivi personali (questa categoria include, ma non si limita a, computer portatili, dispositivi mobili come smartphone e tablet) per svolgere attività lavorative.

2. Il Comune di Cremona non richiede ai suoi dipendenti, collaboratori, amministratori, servizi civile ecc. (“utenti interni”) di utilizzare dispositivi personali per le operazioni lavorative. Tuttavia, riconosce che alcuni utenti possono decidere di utilizzare propri dispositivi per ragioni di comodità, familiarità o efficienza. In risposta a questa tendenza, è stata stabilita la Policy ufficiale BYOD.

3. Il Comune di Cremona non è responsabile e non rimborsa l'acquisto o i costi associati all'uso di dispositivi personali. Gli utenti che scelgono di utilizzare i propri dispositivi per le attività lavorative devono rispettare le linee guida e i requisiti stabiliti in questa Policy per garantire che l'uso dei dispositivi personali avvenga in modo sicuro e responsabile, proteggendo le informazioni sensibili e rispettando le normative sulla privacy e sulla sicurezza dei dati, proteggendo sia l'organizzazione che i suoi utenti da rischi potenziali associati all'uso di dispositivi personali per le attività lavorative.

4. L’autorizzazione all’uso di dispositivi personali per le attività lavorative potrà essere revocata se un utente non rispetta le linee guida e i requisiti stabiliti in questa Policy.

5. Le regole specifiche che gli utenti interni del Comune di Cremona devono seguire, quando utilizzano i propri dispositivi personali per le attività lavorative, sono le seguenti:
   - in nessun momento il dispositivo personale può essere collegato alle reti dell'Ente senza previa autorizzazione;
   - i dispositivi devono soddisfare determinati requisiti di sicurezza: sistema operativo aggiornato, software aggiornato, software antivirus aggiornato. Gli utenti interni sono responsabili dell'aggiornamento dei propri dispositivi personali;
   - prima di utilizzare un dispositivo personale per le attività lavorative, gli utenti devono registrare il dispositivo con il Servizio ICT. Questo processo aiuta a garantire che solo i dispositivi approvati siano utilizzati per accedere alle risorse del Comune di Cremona;
   - gli utenti che scelgono di aderire alla Policy BYOD devono rispettare tutte le regole dell'organizzazione contenute in questo documento;
   - gli utenti non devono memorizzare informazioni personali identificabili o informazioni sensibili del Comune di Cremona sui dispositivi di proprietà personale;
   - gli utenti devono distruggere, rimuovere o restituire tutti i dati, elettronici o meno, appartenenti al Comune di Cremona, una volta terminato il loro rapporto con l'Ente o dopo che non siano più i proprietari o gli utenti principali del dispositivo;
   - gli utenti devono rimuovere o restituire tutte le eventuali licenze di applicazioni software appartenenti al Comune di Cremona quando il dispositivo non viene più utilizzato per le attività lavorative dell'Ente;

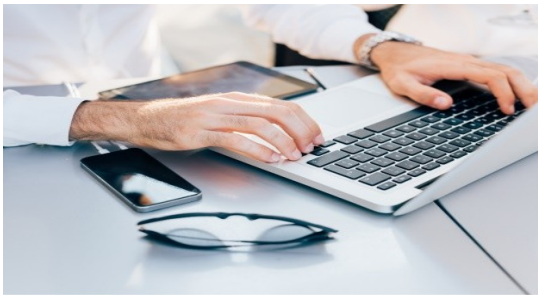
- gli utenti devono notificare al Servizio ICT qualsiasi furto o perdita del dispositivo personale che contiene dati o licenze di applicazioni software appartenenti al Comune di Cremona entro 24 ore;
- Il Comune di Cremona potrà condurre controlli periodici per garantire che i dati personali non siano memorizzati sui dispositivi personali. Questi controlli possono includere audit interni e revisioni dei dispositivi.

Gli utenti interni del Comune di Cremona, che aderiscono alla policy BYOD, devono assumersi le seguenti responsabilità:

- mantenere la sicurezza dei propri dispositivi, inclusa l'installazione di aggiornamenti di sicurezza e software antivirus;
- rispettare tutte le leggi locali e statali;
- proteggere la propria privacy e quella degli altri;
- non memorizzare dati sensibili o personali identificabili dell'Ente sui dispositivi personali;
- rispettare tutte le policy dell'organizzazione relative all'uso delle risorse tecnologiche;
- notificare immediatamente al Servizio ICT in caso di furto o perdita del dispositivo personale;
- accettare che il Comune di Cremona non è responsabile per la manutenzione, il backup o la perdita di dati sul dispositivo personale;
- accettare che il Comune di Cremona non è responsabile per la sicurezza del dispositivo personale quando si accede alle reti dell'Ente;
- accettare che il Comune di Cremona può interrompere la fornitura di risorse IT al dispositivo se il suo uso non è più necessario per le funzioni lavorative;
- accettare che il dispositivo personale può essere soggetto ad analisi e revisione in caso di contenzioso che coinvolge l'Ente;
- accettare che ci sia la registrazione del traffico nelle comunicazioni su Internet e sulla rete dell'Ente, come qualsiasi altro dispositivo aziendale, quando il dispositivo è collegato alla rete dell'Ente;
- accettare che le violazioni di questa policy possono essere rilevate attraverso il monitoraggio di routine dei sistemi di comunicazione elettronica e della rete del Comune di Cremona.

6. In conformità con il GDPR, gli utenti hanno il diritto di accedere, correggere o cancellare i propri dati personali. Per esercitare questi diritti, devono contattare il Responsabile della Protezione dei Dati (DPO).

Art. 15 – Smart Working e collegamenti alla rete interna da remoto



1. Il Comune di Cremona ha attivato la modalità di lavoro Smart Working, attivabile tramite la sottoscrizione di apposito accordo individuale tra il dipendente e il datore di lavoro. Gli utenti dell'Ente interessati a questa modalità possono collegarsi alle risorse informatiche (file, programmi,...) dell'Ente da remoto e in orari flessibili tramite canali sicuri che il Servizio ICT predispone.

2. Per ogni utente che lavora in modalità Smart Working e che necessita di collegarsi alla rete dell'Ente, il Servizio ICT valuta le caratteristiche tecniche della postazione di lavoro remota, del canale di comunicazione tra la postazione remota e la rete del comune e le modalità di fruizione dei software, dei dati e dei file in funzione dei trattamenti che deve fare al fine di consentire l'attività lavorativa in sicurezza e con le flessibilità che lo smart working richiede.
3. Il Servizio ICT, per il collegamento, predilige una soluzione di tipo Virtual Desktop Infrastructure (VDI): una tecnologia che consente di realizzare ambienti desktop disaccoppiati, ovvero in cui i singoli utenti possono visualizzare la propria postazione di lavoro all'interno del comune ed accedendo alle risorse su di essa senza che questi dati escano dall'Ente e vengano a contatto con la postazione remota.
4. La stessa postazione, se di proprietà dell'utente, rimane ad uso privato: non rimarranno su di essa dati e/o software dell'Ente.
5. In fase di avvio dell'attività di Smart Working, il Servizio ICT fornisce le istruzioni per accedere al servizio VDI e per installare sulla postazione remota tutte le componenti necessarie. In caso di necessità l'ICT supporta l'utente nella prima configurazione.
6. Nei casi in cui non possa essere attivata la virtualizzazione del desktop o i trattamenti dei dati richiedono altre modalità, verrà valutata dal Servizio ICT dell'Ente la tecnologia più opportuna per garantire lo svolgere delle attività remote in maniera sicura.

7. Prescrizioni operative:

    1. La postazione di lavoro remota, per collegarsi alla rete dell'Ente, deve rispettare le misure minime di sicurezza espresse dall'Agenzia per l'Italia Digitale (AgID) nella circolare del 18 aprile 2017, n. 2/2017, vale a dire deve:
        - essere protetta da password robusta;
        - essere dotata di sistema operativo aggiornato e supportato;
        - operare con antivirus attivo e aggiornato.

        Tali prescrizioni sono a carico del proprietario della postazione di lavoro.

        Le postazioni che non rispettano le prescrizioni sopra descritte non possono essere utilizzate per attività di Smart Working.
    2. Il Servizio ICT ha facoltà di verificare le prescrizioni operative richieste in fase di attivazione di una postazione remota e successivamente a propria discrezione.
    3. Il Servizio ICT garantisce assistenza solo per quanto riguarda il sistema VDI ed eventuali certificati per il collegamento alla risorse dell'Ente. La manutenzione hardware e software della postazione di lavoro personale è a carico del proprietario, fatti salvi i casi in cui la postazione è di proprietà dell'Ente.
    4. Quando l'utente è in modalità smart working utilizza risorse informatiche di proprietà dell'Ente che lasciano traccia degli accessi e del relativo uso. In caso di sospette violazioni, il Comune di Cremona può verificare tali informazioni, per il tramite dell'Amministratore di Sistema, secondo modalità conformi alla normativa vigente e alle disposizioni del Garante per la protezione dei Dati Personali, nel rispetto dei principi generali di trasparenza, liceità, correttezza, integrità e riservatezza. La tipologia delle informazioni tracciate, le condizioni e le modalità di verifica sono identiche a quelle relative alle postazione di lavoro interne all'Ente.

        Quando l'utente utilizza la postazione di lavoro in modalità privata (no smart working) nessuna attività può essere tracciata dall'Ente. Non ci sono né dotazioni tecniche per farlo né interesse.

5. L’utente che sta operando su dati e programmi dell’Ente, in modalità smart working è tenuto a scollegarsi dal sistema, o bloccare l’accesso (CTRL-ALT-CANC), ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la postazione di lavoro (PC o portatile) o nel caso ritenga di non essere in grado di presidiare l’accesso alla medesima: lasciare un PC incustodito può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.
6. Il Servizio ICT del Comune di Cremona ha sempre la facoltà di intervenire opportunamente sulle limitazioni imposte alle postazioni di lavoro esterne al fine di garantire la sicurezza delle informazioni, dei dati e dei sistemi. Potrà per esempio limitare sulle postazioni VDI l’uso di chiavette e altri supporti esterni o lo scambio di file tra la postazione VDI e il pc personale dell’utente.

Art. 16 – Controlli sugli Strumenti

1. Alla luce dell’art. 4, comma 1, L.n. 300/1970, la regolamentazione della materia indicata nell’art. 1 della presente Policy, non è finalizzata all’esercizio di un controllo a distanza dei lavoratori da parte del datore di lavoro, ma solo a permettere a quest’ultimo di utilizzare sistemi informativi per fare fronte ad esigenze produttive od organizzative e di sicurezza nel trattamento dei dati personali.
   È garantito al singolo lavoratore il controllo sui propri dati personali secondo quanto previsto dagli articoli 15-16-17-18-20-21-77 del Reg. 679/16.
2. Poiché in caso di violazioni contrattuali e giuridiche, sia l’Ente, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, l’Ente verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l’integrità del proprio sistema informatico. Il datore di lavoro, infatti, può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori (art.4, comma 1), di sistemi che consentono indirettamente il controllo a distanza (c.d. controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori. Resta ferma la necessità di rispettare le procedure di informazione e di consultazione di lavoratori e sindacati in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati. I controlli devono essere effettuati nel rispetto del successivo comma del presente articolo e dei seguenti principi:
   1. **Proporzionalità:** il controllo e l’estensione dello stesso dovrà rivestire, in ogni caso, un carattere adeguato, pertinente e non eccessivo rispetto alla/alle finalità perseguite, ma resterà sempre entro i limiti minimi.
   2. **Trasparenza:** l’adozione della presente Policy ha l’obiettivo di informare gli utenti sui diritti ed i doveri di entrambe le parti.
   3. **Pertinenza e non eccedenza:** ovvero evitando un’interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, così come la possibilità di controlli prolungati, costanti o indiscriminati.
3. L’uso degli Strumenti Informatici dell’Ente può lasciare traccia delle informazioni sul relativo uso, come analiticamente spiegato negli art. 5 - 6 - 7 - 8 della presente Policy. Tali informazioni, che possono contenere categorie particolari di dati personali dell’utente, possono essere oggetto di controlli da parte dell’ente, per il tramite

dell'Amministratore di Sistema, volti a garantire esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente, nonché per la sicurezza e la salvaguardia del sistema informatico, per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento / sostituzione / implementazione di programmi, manutenzione hardware, etc.). Gli interventi di controllo sono di due tipi (di seguito descritti al punto i. e ii.) e possono permettere all'Ente di prendere indirettamente cognizione dell'attività svolta con gli strumenti.

i. Controlli per la tutela del patrimonio dell'ente, nonché per la sicurezza e la salvaguardia del sistema informatico. Controlli per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, ecc.).

Qualora per le finalità qui sopra descritte risulti necessario l'accesso agli Strumenti e alle risorse informatiche e relative informazioni descritte agli art. 5 - 6 - 7 - 8 il Responsabile del trattamento dei dati personali per il tramite dell'Amministratore di Sistema, si atterrà al processo descritto qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo).

a) Avviso generico a tutti i dipendenti della presenza di comportamenti anomali che possono mettere a rischio la sicurezza del sistema informativo e richiamo all'esigenza di attenersi al rispetto della presente Policy.
b) Successivamente, dopo almeno 7 giorni, se il comportamento anomalo persiste, l'ente potrà autorizzare il personale addetto al controllo, potendo così accedere alle informazioni descritte ai punti 5 - 6 -7 - 8 con possibilità di rilevare file trattati, siti web visitati, software installati, documenti scaricati, statistiche sull'uso di risorse ecc. nel corso dell'attività lavorativa. Tale attività potrà essere effettuata in forma anonima ovvero tramite controllo del numero IP, dell'utente e con l'identificazione del soggetto che non si attiene alle istruzioni impartite.
c) Qualora il rischio di compromissione del sistema informativo dell'ente sia imminente e grave a tal punto da non permettere l'attesa dei tempi necessari per i passaggi procedimentali descritti ai punti a) e b), il Responsabile del Trattamento, unitamente all'Amministratore di Sistema, può intervenire senza indugio sullo strumento da cui proviene la potenziale minaccia.

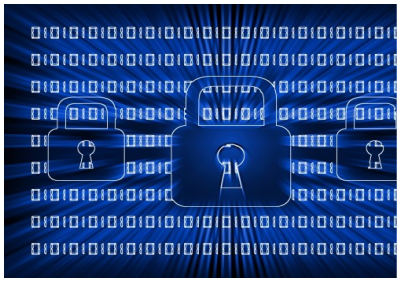
ii. Controlli per esigenze produttive e di organizzazione

Per esigenze produttive e di organizzazione si intendono – fra le altre – l'urgente ed improrogabile necessità di accedere a file o informazioni lavorative di cui si è ragionevolmente certi che siano disponibili su risorse informatiche di un utente che non sia reperibile, in quanto ad esempio assente, temporaneamente irreperibile ovvero cessato. Qualora risulti necessario l'accesso alle risorse informatiche e relative informazioni descritte agli artt. di cui ai punti 5 - 6 - 7 - 8 il Responsabile del trattamento dei dati personali, per il tramite dell'Amministratore di Sistema, si atterrà alla procedura descritta qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo).

a) Redazione di un atto da parte del Responsabile del Servizio che comprovi le necessità produttive e di organizzazione che richiedano l'accesso allo Strumento.
b) Incarico all'Amministratore di sistema di accedere alla risorsa con credenziali di Amministratore ovvero tramite l'azzeramento e la contestuale creazione di nuove credenziali di autenticazione dell'utente interessato, con avviso che al primo accesso alla risorsa, lo stesso dovrà inserire nuove credenziali.
c) Redazione di un verbale che riassuma i passaggi precedenti.

d) In ogni caso l'accesso ai documenti presenti nella risorsa è limitato a quanto strettamente indispensabile alle finalità produttive e di organizzazione del lavoro.

Art. 16.1 – Conservazione dei dati



1. In riferimento agli articoli 5 e 6 del Reg. 679/16 e in applicazione ai principi di diritto di accesso, legittimità, proporzionalità, sicurezza accuratezza e conservazione dei dati, le informazioni relative all'accesso ad Internet e dal traffico telematico (log di sistema e del server proxy), la cui conservazione non sia definita necessaria, saranno trattati come indica il garante e quindi cancellati dopo un periodo di sei mesi.
2. In casi eccezionali, ad esempio per esigenze tecniche o di sicurezza o per l'indispensabilità dei dati rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria o, infine, all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria, è consentito il prolungamento dei tempi di conservazione limitatamente al soddisfacimento delle esigenze sopra esplicitate.
3. L'Ente si impegna ad applicare le misure di sicurezza nel trattamento e nella conservazione di tale tipologia di dati alla luce di quanto stabilito dal Legislatore.

Art. 17 - Sanzioni Disciplinari

1. È fatto obbligo a tutti i dipendenti di osservare le disposizioni della presente Policy. Eventuali violazioni comportano, a seconda della gravità dell'infrazione, l'adozione dei provvedimenti disciplinari in ragione del richiamo fatto dal codice di comportamento del Comune di Cremona alle disposizioni introdotte dall'Amministrazione nella materia oggetto della corrente Policy.
2. Il Comune di Cremona riserva il diritto di intraprendere azioni civili e penali nei confronti dei responsabili di danni all'Ente.

Allegato A)

TERMINOLOGIA

TERMINE	SPIEGAZIONE
AGID	L'Agenzia per l'Italia Digitale è l'agenzia tecnica della Presidenza del Consiglio che ha il compito di garantire la realizzazione degli obiettivi dell'Agenda digitale italiana e contribuire alla diffusione dell'utilizzo delle tecnologie dell'informazione e della comunicazione, favorendo l'innovazione e la crescita economica. AgID ha il compito di coordinare le amministrazioni nel percorso di attuazione del Piano Triennale per l'informatica della Pubblica amministrazione, favorendo la trasformazione digitale del Paese. AgID sostiene l'innovazione digitale e promuove la diffusione delle competenze digitali anche in collaborazione con le istituzioni e gli organismi internazionali, nazionali e locali.
Autenticazione informatica	L'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità, per esempio l'insieme di nome utente e password ovvero l'utilizzo di smart card o badge di identificazione ai sistemi: • **"credenziali di autenticazione"**, i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica; • **"parola chiave"**, componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica; • **"profilo di autorizzazione"**, l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti.
Autorizzazione	Un provvedimento adottato dal Garante, grazie al quale un Titolare può essere autorizzato a trattare determinati dati personali e/o giudiziari ed a trasferire dati personali all'estero. In altri casi è da intendersi come autorizzazione ad accedere ad un applicativo.
Banca di dati	Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti. Anche in questo caso, si faccia attenzione al fatto che la legge non pone alcuna differenza fra una banca di dati realizzata su schede cartacee, piuttosto che archiviata in un sistema informatizzato.
Cloud Service Provider (CSP)	I provider di servizi cloud sono aziende che forniscono servizi di infrastruttura, piattaforme e/o software tramite una rete. Rivolgersi a un provider di servizi cloud è un modo per accedere a servizi di elaborazione senza che l'Ente debba acquistare risorse quali: infrastruttura, piattaforme, software.
Comunicazione elettronica	Ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico.
Dominio di Rete	Un dominio è una rete di computer, tipicamente una LAN di un'organizzazione ove la logica client-server è supportata, oltre che da connessioni fisiche e relativi protocolli anche da regole (*policy*) di connessione logica di tipo autorizzativo (regole di sicurezza). In questo contesto, un client deve sottostare a procedure di autenticazione specifiche, definite da servizi che risiedono su un server. Queste procedure, che solitamente sottendono una gerarchia di profili (in termini di permessi e accessi alle risorse o ai sistemi), determinano l'appartenenza o meno al dominio, struttura di distribuzione e condivisione centralizzata.
Firewall	Un prodotto hardware e software in grado di controllare lo scambio di comunicazioni tra una Rete ad esso esterna, la zona non protetta, ed una Rete ad esso interna, la zona protetta, in ambiente Internet.

TERMINE	SPIEGAZIONE
Informazioni Personali Identificabili (IPI)	Questo termine si riferisce a qualsiasi informazione che può essere utilizzata per identificare un individuo. Le IPI possono includere, ma non sono limitate a, nome, numero di previdenza sociale, data e luogo di nascita. Le IPI possono anche includere qualsiasi altra informazione che è collegata o collegabile a un individuo.
LAN	**Local Area Network** (**LAN**) (in italiano **rete in area locale**, o **rete locale**), in informatica e telecomunicazioni, indica una rete informatica di collegamento tra più computer, estendibile anche a dispositivi periferici condivisi, che copre un'area limitata, come un'abitazione, una scuola, un'azienda o un complesso di edifici adiacenti.
Password Manager	Programmi e app che archiviano in modo sicuro e crittografato le credenziali (username e password) di accesso ai servizi web (e non solo) in una sorta di cassaforte ("Vault") virtuale, rendendola disponibile all'utente quando ne avrà bisogno. Sono protetti da una **Master Password**, che serve per aprirli e diventa perciò l'**unica** password che occorre ricordare (con lo svantaggio che se non viene ricordata non si può accedere al PM).
Phishing	Il **phishing** è un tipo di truffa effettuata su Internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale.
Protezione Antivirus Aggiornata	Si riferisce a un software antivirus che è stato aggiornato con le definizioni più recenti. Queste definizioni permettono al software di rilevare e neutralizzare le minacce più recenti alla sicurezza dei dati. Per garantire una protezione efficace, il software antivirus deve essere aggiornato regolarmente, preferibilmente ogni giorno
Salvataggio dei dati	Operazione di "messa in conserva" e riparo dei dati informatici e non.
Screenshot	File di immagine contenente una fotografia della schermata presente sul computer.
Servizio ICT e Agenda Digitale	O abbreviato Servizio ICT è il Servizio Interno al Comune di Cremona, Area Risorse e Servizi di Staff, Unità Direzionale Segretario Generale, che si occupa delle risorse informatiche dell'Ente.
Servizi Informatici	Servizio esterno o interno avente il compito di mantenere in efficienza la Rete Informatica ed il patrimonio tecnologico dell'ente.
Software as a Service (SaaS)	E' un modello di licenza e distribuzione del software utilizzato per fornire applicazioni su Internet come servizio.
Spamming	Lo ***spamming***, detto anche **fare spam** o **spammare**, è l'invio anche verso indirizzi generici, non verificati o sconosciuti, di messaggi ripetuti ad alta frequenza o a carattere di monotematicità tale da renderli indesiderati (generalmente commerciali o offensivi) ed è noto anche come **posta spazzatura.**

TERMINE	SPIEGAZIONE
Strumenti elettronici	Gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento. Si badi al fatto che la legge è volutamente generica nella descrizione degli strumenti elettronici, perché vuole che il Titolare e Autorizzato al trattamento si rendano conto del fatto che già oggi i dati personali possono essere archiviati nei supporti più disparati, come ad esempio stick memory, le smart card di una macchina fotografica digitale, la memoria buffer di una stampante, il server di un sistema di posta elettronica, dove i messaggi vengono archiviati in attesa di essere letti dal destinatario, e via dicendo.
TCP/IP	Trasmission Control Protocol/Internet Protocol: un protocollo di trasmissione via Internet.
Web	Letteralmente, ragnatela - Abbreviazione di www (Wolrd Wide Web).
Wi Fi	Wireless Fidelity: nome di una tecnologia, inquadrata nello standard internazionale IEEE 802.11 b, utilizzata per reti locali senza fili, che lavora nella banda 2,4 GHz e con rateo di trasmissione dell'ordine di 10 MBps.
VLAN	Virtual Local Area Network (Rete Locale Virtuale). Con gli switch moderni si riescono a costruire lan virtuali (vlan), cioè insiemi di macchine che si comportano come se fossero reti separate (quindi non condividono i broadcast), e che possono essere composte da macchine collegate a uno o più switch, comunque distribuite all'interno dell'ente. Concettualmente si parla di *Dominio di Broadcast*.