gennaio 2020

Linee Guida per l'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).
   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.
   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).
   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).
   La Posta Elettronica Certificata (PEC), molto simile alla posta elettronica, 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 dati relativi a categorie particolari di dati personali. Essendo però una tipologia di servizio non comune (e in molti casi a pagamento), è meno diffusa della posta elettronica ordinaria, e di solito limitata ad un uso professionale.

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.

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.

Prescrizioni operative:

2. Ad ogni utente viene fornito un account e-mail nominativo, generalmente coerente con il modello nome.cognome@comune.cremona.it. L'utente a cui è assegnata una casella di posta elettronica è responsabile del corretto utilizzo della stessa. La gestione dell'account dovrà rispondere ai seguenti criteri di robustezza e di scadenza:

   - La password deve essere composta da almeno 8 caratteri, formata da lettere maiuscole e minuscole, da almeno un numero e da almeno un carattere speciale (!_?/- ecc.). Non deve contenere riferimenti agevolmente riconducibili all'utente (username, nomi o date relative alla persona o ad un famigliare). In caso di inserimento di una password errata è possibile effettuare fino a 5 tentativi dopodiché l'utenza viene bloccata per 30 minuti.

   - È necessario procedere alla modifica della password, a cura dell'utente, al primo accesso e, successivamente, almeno ogni sei mesi. 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.

3. 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.
4. La posta deve essere gestita con il programma Zimbra e con la casella di posta elettronica istituzionale assegnati dal Servizio ICT del Comune di Cremona. Non possono essere usati altri sistemi di posta elettronica, se non espressamente autorizzati e configurati dal Servizio ICT.
5. 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.
6. 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.
7. 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.
8. 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.

9. 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 adeguato avviso automatico relativo alla chiusura della casella, indicando il nuovo indirizzo a cui inviare le email; in caso di impossibilità oggettiva sarà il Servizio ICT ad effettuare l'adempimento.
   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.
10. 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, ai messaggi con allegati file.rar 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.
11. Non é consentito diffondere messaggi del tipo "catena di S. Antonio" o di tipologia simile anche se il contenuto sembra meritevole di attenzione; in particolare gli appelli di solidarietà e i messaggi che informano dell'esistenza di nuovi virus. In generale è vietato l'invio di messaggi pubblicitari di prodotti di qualsiasi tipo.
12. 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.
13. 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.
14. 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.
15. È vietato inviare posta elettronica in nome e per conto di un altro utente, salvo sua espressa autorizzazione.
16. 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.

17. 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 in 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.

18. Si informa che 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.