COMUNE DI
REGGIO NELL'EMILIA

Reggio Emilia
città
delle persone

DISCIPLINARE
PER UTENTI DEI SISTEMI INFORMATIVI

Sommario

1. Introduzione

Il presente disciplinare descrive le regole tecniche ed organizzative da applicare per l'utilizzo di strumentazioni informatiche che accedono al sistema informativo del Comune di Reggio nell'Emilia, di seguito denominato "Ente".
Ai fini del presente disciplinare, si intende per "sistema informativo" il complesso dei dati, delle applicazioni, delle risorse tecnologiche, delle risorse umane, delle regole organizzative e delle procedure deputate alla acquisizione, memorizzazione, consultazione, elaborazione, conservazione, cancellazione, trasmissione e diffusione delle informazioni.
Le disposizioni qui contenute hanno la finalità di ottimizzare l'impiego delle risorse, introdurre regole di corretto utilizzo nel contesto organizzativo dell'Ente e ridurre al minimo i rischi di distruzione o perdita anche accidentale dei dati e delle informazioni, di accesso non autorizzato o di trattamento non consentito, garantire la disponibilità dei servizi e il rispetto delle norme sul diritto d'autore.
Quanto riportato nel presente disciplinare non esaurisce tutte le prescrizioni contenute nelle vigenti normative relativamente ad illeciti disciplinari, civili e penali, con particolare riferimento alle violazioni di sicurezza e ai reati informatici.

2. Campo di applicazione

Il presente disciplinare si applica a tutti i soggetti che utilizzano i servizi del sistema informativo dell'Ente il cui accesso è consentito tramite credenziali personali.
Il presente disciplinare non riguarda le dotazioni informatiche dei plessi scolastici gestiti dall'Istituzione Nidi e Scuole d'infanzia del Comune di Reggio Emilia installate presso le strutture delle singole scuole e gestite direttamente dal personale tecnico del Servizio medesimo.
Il presente disciplinare si applica anche ai dipendenti dell'Istituzione scuole e Nidi d'infanzia per tutte le modalità operative e comportamentali ivi contenute.

3. Dotazioni informatiche individuali

In relazione al rapporto di lavoro instaurato e alle mansioni affidate, il Comune di Reggio Emilia assegna agli utenti una postazione di lavoro per l'accesso alla rete e ai servizi del sistema informativo, ovvero un insieme di dotazioni software aziendali (comprese le stampanti multifunzione), con configurazione predisposta per assicurare la riservatezza dei dati personali e delle informazioni trattate.
Per collaboratori esterni che abbiano necessità di accedere ai servizi del sistema informativo dell'Ente, l'assegnazione di strumentazione idonea viene valutata dal Dirigente del Servizio Informatica di concerto con il responsabile della UOC Gestione Strutture Tecnologiche.
Ogni utente è responsabile del corretto impiego delle risorse messe a sua disposizione dall'Ente.

3.1 Postazioni di lavoro

La tipologia e le caratteristiche delle postazioni di lavoro sono stabilite dal Servizio informatica, tenuto conto delle esigenze di lavoro rilevate per gruppi di utenti omogenei, dell'evoluzione tecnologica e del rapporto qualità/prezzo/efficienza delle tecnologie disponibili.
Le postazioni di lavoro hanno caratteristiche minime comuni costituite da:

- un sistema operativo omogeneo e sicuro;
- una dotazione di applicativi individuali di base omogenei e standardizzati;
- un insieme di tecnologie che abilitano all'accesso alla rete e a tutti i servizi applicativi dell'Ente, compresi eventuali certificati e/o dispositivi per il controllo delle identità del dispositivo e dell'utente;
- la possibilità di accesso da parte di Amministratori di Postazioni di Lavoro (PdL) per l'erogazione dei servizi di assistenza remota e aggiornamento automatico;
- configurazione parametri standardizzati definiti centralmente ai fini di garantire la sicurezza della postazione stessa.

Qualora siano necessarie dotazioni aggiuntive (ad esempio l'installazione di un doppio monitor) il Dirigente del Servizio richiedente dovrà effettuare richiesta scritta adeguatamente motivata al Dirigente del Servizio Informatica. La richiesta dovrà comunque essere autorizzata dal Dirigente del Servizio Informatica previe verifiche tecniche ed economiche.

Le postazioni di lavoro sono protette, in caso di assenza anche temporanea, tramite la sospensione o il blocco della sessione di lavoro. A tale fine è impostata automaticamente l'attivazione dello screen saver in un periodo di tempo congruo e definito dal Servizio Informatica al fine di impedire la lettura e/o la modifica dei dati presenti a video.
Allo scopo di proteggere dati personali di cui il Comune di Reggio Emilia è titolare e di salvaguardare la sicurezza delle postazioni di lavoro, è vietato collegare supporti rimovibili o altre tipologie di dispositivi di proprietà dell'utente alle postazioni di lavoro dell'Ente.

3.2 Dotazione software della postazione di lavoro individuale

Ogni postazione di lavoro è dotata di una configurazione base costituita da un set di software applicativi (Vedi Allegato A_Elenco Software Standard PdL)
La postazione di lavoro è configurata e gestita centralmente dagli Amministratori di PdL nel rispetto del principio delle policies di standardizzazione di tutte le postazioni di lavoro del Comune di Reggio Emilia, definite dal Servizio Informatica.
Qualora siano necessarie dotazioni software aggiuntive il Dirigente del servizio richiedente dovrà effettuare richiesta scritta adeguatamente motivata al Dirigente del Servizio Informatica. La richiesta dovrà comunque essere autorizzata dal Dirigente del Servizio Informatica previe verifiche dei requisiti di sicurezza, della sostenibilità gestionale, della economicità e idoneità funzionale. Come criterio generale si dovranno privilegiare software:

- open source, a riuso;
- che non prevedano costi di acquisizione / mantenimento ;
- che consentano una gestione centralizzata dell'installazione/aggiornamento;
- che presentino le adeguate garanzie di sicurezza a protezione dei dati personali in ottemperanza all'articolo 32 del Regolamento europeo 679/2016.

E' ASSOLUTAMENTE VIETATO installare qualunque tipo di software (inclusi estensioni del browser, plug-in, portable, ecc.) o modificare configurazioni rilevanti del sistema operativo (ad es: impostazioni scheda di rete, ecc.) senza il consenso del Servizio Informatica.

3.3 Fotocopia e scanner

Tutti gli utenti del Comune di Reggio Emilia possono accedere alle stampanti/copiatrici multifunzione, indipendentemente dalla loro collocazione fisica. Tali stampanti sono gestite dal server centrale di controllo dei servizi di stampa e copia che garantisce i principi di stampa sicura al fine della tutela dei dati personali.
La parte di scansione di questi dispositivi multifunzione è configurata in modo da avere due destinazioni per i file scansionati, ognuna delle quali ha un sistema di disponibilità dei dati diversa:

- Scansione su disco di servizio I:\SCANSIONI, dati disponibili per 7 giorni
- Scansione su disco Y:\, dati disponibili per 1 giorno

La destinazione del percorso di scansione viene decisa dall'utente direttamente sul pannello del dispositivo durante la fase di scansione. Nel caso in cui la stampante sia ad uso di più servizi, sul display della stampante è sempre presente l'opzione di scelta tra i Servizi disponibili, oltre alla possibilità di scansione su disco Y.
Per particolari necessità i Dirigenti dei Servizi possono richiedere la creazione sul disco I:\ di cartelle di scansione con diritti d'accesso circoscritti ad alcune persone. Anche in questo caso verrà creata dal Servizio informatica un'apposita opzione sul pannello della stampante.

3.4 Corretto utilizzo e conservazione delle dotazioni di lavoro

Le dotazioni informatiche di lavoro, insieme agli accessori fisici e alle dotazioni software individuali, devono essere:

- consegnate ad ogni nuovo utente con la configurazione standard di base aggiornata alla data di consegna;
- utilizzate e conservate con diligenza al fine di ottimizzare l'impiego delle risorse dell'Ente, il risparmio energetico e l'impatto ambientale, nel rispetto del presente Disciplinare;
- mantenute collegate alla rete, con particolare riferimento al dispositivi notebook (vedi par. 5)
- protette da eventuali accessi indesiderati. Le postazioni sono programmate per bloccarsi dopo 20 minuti di inattività. Se l'utente si assenta dall'ufficio e lascia incustodita la postazione di lavoro prima che si verifichi il blocco automatico, è necessario che l'utente blocchi manualmente la postazione attraverso la sequenza di comandi "ALT+CTRL+CANC" per evitare che altri soggetti possano accedervi utilizzando le credenziali ad insaputa del soggetto proprietario;
- utilizzate in modo pertinente alle specifiche finalità della propria attività e di quelle della propria organizzazione, nel rispetto delle esigenze di funzionalità e sicurezza dei sistemi informativi;
- custodite, anche in caso di trasferimento di sede e struttura dell'utente, insieme a tutte le altre dotazioni strumentali personali;
- restituite immediatamente in caso di cessazione del rapporto di lavoro e/o collaborazione;

Per ridurre i consumi elettrici gli utenti devono provvedere a spegnere il proprio monitor, stampanti e/o altri dispositivi non dotati di spegnimento automatico e risparmio energetico al termine dell'orario di lavoro. Tutte le postazioni sono impostate centralmente per uno spegnimento automatico alle ore 20.00 sette giorni su sette. Nei casi in cui, per esigenze di servizio, sia necessario modificare in modo permanente o in situazioni particolari questa regola per la singola postazione o per un gruppo di postazioni, è necessario aprire un ticket di assistenza indicando il/i nomi delle postazioni su cui intervenire con almeno due giorni di anticipo.

I dati e le informazioni trattati devono essere salvati nei percorsi di rete assegnati su cui viene garantito il back-up con le seguenti modalità:

- copia tutte le notti
- mantenimento della copia per 3 mesi

che consentono di ripristinare documenti cancellati entro gli ultimi 3 mesi.

Non viene effettuato nessun tipo di back-up su dati salvati sui dischi locali della postazione (C: D:) o su eventuali dischi removibili esterni anche se autorizzati e di proprietà dell'Ente (il cui utilizzo, anche per questa ragione, è fortemente sconsigliato); pertanto in caso di cancellazione accidentale o di danneggiamento del supporto magnetico non sarà possibile recuperarli.
Come misura di sicurezza a protezione dei dati personali è vietato salvare dati personali sia di natura identificativa che di natura particolare di cui l'Ente è titolare sui dischi locali della postazione di lavoro o su dischi removibili (vedi chiavette USB) anche se di proprietà dell'Ente. In caso di necessità di salvare dati personali e particolari sui dischi di rete in modo

che siano accessibili solo a gruppi di personale autorizzato e non a tutti coloro che accedono al disco di rete del Servizio, sarà necessario che il Dirigente coordinatore del trattamento dei dati invii richiesta scrivendo a: callcenter@comune.re.it indicando il nome della cartella, le persone autorizzate ad accedervi e con quale modalità (lettura o scrittura).

Si tenga presente che la richiesta può essere fatta solo per cartelle di primo livello del disco e della cartella di UOC, qualora siano previste dalla struttura organizzativa (ad esempio: I:\ nome_cartella o I:\UOCxxxxx\Nome_Cartella).

In caso sia indispensabile salvare temporaneamente dati personali o particolari su dischi locali o su supporti removibili di proprietà dell'Ente si dovranno utilizzare accorgimenti che li rendano inaccessibili a terzi, come ad esempio:

- proteggere il documento con una password
- creare una cartella compressa (.ZIP) protetta con una password di crittografia

In caso di sostituzione o guasto della postazione di lavoro, il servizio di Help Desk effettuerà, ove possibile, operazioni di salvataggio di dati e informazioni salvati sui dischi locali della postazione.

Le dotazioni restituite, ritirate per riparazione o sostituite per aggiornamento della dotazione, vengono immediatamente riconfigurate (formattando il disco e reinstallando il sistema operativo e tutti i programmi inclusi nella configurazione standard), in modo da cancellare ogni dato preesistente e riportate alla configurazione standard. Le dotazioni riconfigurate vengono consegnate al Servizio Informatica e rese disponibili per altri utenti.

3.5 Richiesta di assistenza e interventi sulle postazioni di lavoro

Tutte le chiamate di assistenza per:

- problemi sulle postazioni di lavoro o sulle periferiche ad esso collegate
- problemi su stampanti di rete
- problemi su accesso ad internet e posta elettronica
- problemi su software installato su tutte le postazioni e/o software applicativo specifico
- richieste di nuove credenziali
- modifica dei diritti di accesso
- aiuto nell'uso degli strumenti informatici
- ecc.

devono essere fatte, salvo diverse indicazioni, tramite apertura di un Ticket di "Assistenza Informatica" accessibile dalla Intranet o dal box presente in alto a destra sul desktop della propria postazione di lavoro.
In alternativa, e solo nel caso in cui il sistema di "Assistenza Informatica" non funzioni, si può inviare una mail a callcenter@comune.re.it

Richieste di assistenza pervenute direttamente ai referenti applicativi o con canali diversi non saranno prese in considerazione.

Ove possibile i tecnici del Servizio informatica o dell'Help Desk, possono collegarsi in modalità remota alla postazione di lavoro, ogni qual volta vi sia la necessità di assicurare l'assistenza tecnica in tempi più veloci, la sicurezza e l'operatività, effettuando operazioni di manutenzione e aggiornamento dei software installati. Gli interventi sono effettuati dagli Amministratori di PdL nelle seguenti modalità:

- accedendo alla postazione con proprie credenziali in assenza dell'utente;
- collegandosi in remoto utilizzando la sessione dell'utente connesso, presente e a seguito di suo assenso orale.

Nei casi in cui l'utente segnala malfunzionamenti per la soluzione dei quali, a scopi diagnostici, è indispensabile impersonare l'utente e accedere con i privilegi allo stesso assegnati, l'intervento viene effettuato, solo su specifica richiesta e autorizzazione orale dell'utente stesso.

Le attività di aggiornamento software della postazione vengono generalmente automatizzati e distribuiti durante la notte per ridurre l'impatto sull'operatività degli uffici. In alcuni casi, qualora non fosse possibile effettuare l'aggiornamento in orario notturno, tali aggiornamenti possono essere effettuati durante l'orario lavorativo e può essere richiesto all'utente il riavvio della propria postazione.

Tutte le operazioni di collegamento/distribuzione da remoto vengono fatte tramite la piattaforma Microsoft SCCM che consente di tracciare le attività effettuate.

4. Credenziali di identificazione informatica e attivazione dei servizi

Si delineano di seguito le procedure e le regole d'uso per la gestione e assegnazione delle credenziali di identificazione informatica e le procedure per l'attivazione dei servizi assegnati all'utente.
L'accesso alle strumentazioni informatiche utilizzate per i trattamenti di dati personali è consentito soltanto ai Coordinatori del trattamento dei dati (ovvero i Dirigenti), nominati dal Sindaco, e agli incaricati formalmente nominati dai coordinatori stessi ai sensi dell'articolo 4, punto 10 del Regolamento Europeo 679/2016 in materia di protezione dei dati personali.

4.1 Credenziali di identificazione informatica

L'accesso ai dati trattati con strumentazioni informatiche avviene esclusivamente previa autenticazione.
Le credenziali di identificazione informatica consistono in un codice di 6 caratteri per l'identificazione dell'utente e una parola chiave riservata (Username e Password), conosciuta solamente dal medesimo.
Le credenziali sono nominative e personali mentre la password è temporanea e generata casualmente dagli "account operators", come definiti nel glossario in calce al presente documento.
L'utente, al primo log-on, viene obbligato dalla procedura di autenticazione a cambiare la password inizialmente assegnata.

Le credenziali di accesso abilitano l'utente a:

- accesso ad internet/intranet
- accesso al disco di rete I: del proprio servizio
- accesso alle directory su cui si e' abilitati del disco M:
- eventuale accesso a dischi di rete di altri servizi a cui si è abilitati
- accesso alla propria casella di posta
- accesso ad applicazioni a cui si e' stati autorizzati (vedi paragrafo successivo)

Per evitare il prolificare delle credenziali, con le stesse credenziali, ove tecnicamente consentito, è possibile accedere ad applicazioni diverse (es: intranet, posta, Jente, ecc.). Questa modalità rende quindi molto importante il rispetto delle regole per la gestione delle credenziali indicate nel par. 4.4 in quanto la compromissione della password potrebbe consentire l'accesso ad applicazioni critiche e/o contenenti dati personali e /o particolari determinando un danno rilevante per l'amministrazione.

4.2 Assegnazione delle credenziali al personale e agli organi politici dell'Ente

Il rilascio delle credenziali di identificazione informatica al personale dell'Ente (compresi i tempi determinati e il personale comandato o in avvalimento da altre strutture pubbliche presso l'Ente), agli organi politici (Sindaco, Consiglieri e Assessori), è conseguente alla procedura di inquadramento giuridico da parte del Servizio competente.
Il processo di rilascio delle credenziali informatiche è di competenza del Servizio Informatica a seguito di formale richiesta scritta da parte dell'Ufficio Personale in caso di utenza dipendente, o direttamente dal dirigente del Servizio assegnatario in caso di incaricati esterni. Il processo di autorizzazione all'accesso ai sistemi e l'assegnazione di ruoli, così come la modifica e la revoca, viene eseguito dal Servizio Informatica a seguito di formale richiesta scritta da parte del Dirigente competente o dall'Ufficio Personale.
Le credenziali di identificazione informatica sono concesse, in base alla tipologia, (DIPENDENTE o NON DIPENDENTE) attraverso il seguente iter pubblicato nella intranet del Comune che di seguito integralmente si riporta:

1. **Iscrivere un nuovo utente DIPENDENTE alla rete informatica**
   A chi è necessario rivolgersi?
   La richiesta va inoltrata dal Dirigente del Servizio, aprendo una chiamata su HDM al link Assistenza Informatica
   Quali sono le informazioni da comunicare?
   - Nome e Cognome del nuovo utente , data e luogo di nascita
   - Codice fiscale dell'interessato , controllare attentamente i dati trasmessi
   - Servizio di appartenenza
   - Ufficio e recapito telefonico
   - Elenco cartelle di rete a cui può accedere il nuovo utente, specificando il tipo di accesso permesso (sola lettura/lettura e scrittura)
   - Elenco delle procedure che dovrà utilizzare
   - Specificare se l'utente ha diritto solo nella Intranet o anche in Internet.

   N.B. Se il nuovo utente ha un contratto a **tempo determinato** indicare la data di scadenza del contratto. **In caso la persona sia esterna all'ente, e non abbia quindi un contratto a tempo determinato o indeterminato, fare riferimento alla FAQ "Richiesta abilitazioni persone esterne"**
   Qualora il dirigente voglia autorizzare il nuovo utente alla consultazione dell'anagrafe, oltre all'ufficio scrivente, deve indirizzare la richiesta, almeno per conoscenza, al Dirigente del Servizio competente

2. **Trasferire un utente della Rete Informatica da un servizio ad un altro**
   A chi è necessario rivolgersi?
   E' necessario aprire una chiamata su HDM al link Assistenza Informatica. La richiesta va inoltrata dal Dirigente del Servizio in cui dovrà essere trasferito l'utente.
   Quali informazioni devono essere comunicate?
   - Nome e Cognome del nuovo utente

- Servizio di provenienza e Servizio di arrivo
- Nuovo Ufficio
- Nuovo recapito telefonico
- Elenco cartelle di rete a cui può accedere l'utente, specificando il tipo di accesso permesso (sola lettura/lettura e scrittura)
- Elenco delle procedure che dovrà utilizzare
- Specificare se l'utente ha diritto solo nella Intranet o anche in Internet

N.B. **Anche se nel settore di provenienza l'utente aveva accesso ad Internet, con il trasferimento perde automaticamente il diritto alla navigazione, perciò deve ottenere l' autorizzazione dal nuovo Dirigente del Servizio**.

3. **Come richiedere l'accesso alla rete per personale ESTERNO non DIPENDENTE**
   Per richiedere l'abilitazione, la disattivazione, la proroga o la modifica dell'accesso alla rete dell'ente per PERSONALE ESTERNO NON ASSUNTO A TEMPO DETERMINATO O INDETERMINATO occorre compilare il modulo allegato.
   Si tratta di un modello pdf che deve **essere compilato sul pc** per ciascuna persona che deve utilizzare i servizi di rete, **firmato digitalmente dal dirigente** del servizio di riferimento e da eventuali dirigenti di altri servizi che hanno la titolarità di dati/procedure a cui si richiede l'accesso.
   Il documento va inviato, insieme alla copia scannerizzata dell'atto che norma l'attività della persona presso l'ente, a **rinnovoutenti@municipio.re.it almeno 1 settimana prima** rispetto a quando l'accesso dovrà essere attivo.
   Come indicato nel documento stesso, qualora l'atto non sia ancora ufficializzato, la proroga può essere richiesta per un periodo massimo di 6 mesi dalla scadenza prevista dall'ultimo atto comunicato.
   Naturalmente, in caso l'atto sia già presente in formato digitale (ad esempio all'interno di jente) basta inviare il PDF (vedi Allegato B_richiesta accesso personale Esterno)

Le credenziali di identificazione informatica sono associate ai dati con cui il personale è registrato nell'anagrafica dell'Ente e costituiscono condizione necessaria per l'abilitazione all'utilizzo dei servizi informatici.

4.3 Assegnazione delle credenziali a soggetti esterni

Qualsiasi soggetto esterno che debba accedere ai servizi di rete e di dominio direttamente presso le sedi del Comune di Reggio Emilia o accedere tramite VPN da remoto a sistemi della rete interna, indipendentemente dall'inquadramento giuridico e/o dalla forma diretta o indiretta del proprio rapporto di collaborazione, deve essere accreditato tramite il rilascio di una credenziale informatica nominativa. Il processo di rilascio delle credenziali segue quanto indicato nel paragrafo precedente.
La richiesta di accreditare un soggetto esterno avviene su istanza del Dirigente del Servizio di assegnazione del soggetto. La richiesta di accreditamento dovrà riportare per ogni soggetto da accreditare i minimi dati necessari per il rilascio delle credenziali incluso il termine di accreditamento.

Il rilascio delle credenziali avviene su disposizione del Dirigente del Servizio Informatica o suo delegato.

Si possono distinguere due categoria principali di utenze esterne:

- utenti generalmente dipendenti di altri Enti che per necessità istituzionali devono accedere ad applicazioni dell'ente accessibili da web (vedi "Allegato C_Risorse accedibili dall'Esterno"): in questo caso la richiesta di accesso dovrà pervenire dal Dirigente Coordinatore del trattamento dei dati che avrà l'onere delle verifiche di ammissibilità della richiesta e dovrà indicare l'applicazione ed i ruoli che dovranno essere assegnati;
- utenti generalmente collaboratori di software house che per attività di manutenzione devono collegarsi a sistemi non accessibili da internet. In tal caso a seguito della valutazione tecnica del responsabile della UOC Gestione Strutture tecnologiche, la ditta per cui l'utente opera dovrà sottoscrivere a seconda dei casi:
  a) se la tipologia di accesso richiesta rientra nella casistica di Amministratore di Sistema, la nomina ad Amministratore di Sistema corredata da formale attestazione inerente la corrispondenza alle caratteristiche di esperienza, capacità e affidabilità del soggetto designato richieste dalla normativa (cfr. Provvedimento Garante per la protezione dei dati personale del 27/11/2008).
  b) se la tipologia di accesso rientra nella casistica di Responsabile Esterno del Trattamento ai sensi dell'Art.28 del Regolamento UE 679/2016, apposito addendum contrattuale contenente le indicazioni a tutela dei dati personali trattati che il Titolare fornisce al Responsabile del trattamento.
- Nei casi a) e b) sopra riportati, oltre ai documenti contrattuali citati precedentemente, saranno richieste con separato documento che dovrà essere sottoscritto dal legale rappresentante della ditta/società/software house le seguenti informazioni:
  - le finalità per cui si richiede l'accesso;
  - i sistemi e i protocolli a cui si richiede l'accesso;
  - l'elenco delle persone autorizzate all'accesso con indicazione del codice fiscale ed email nominativa;
  - riferimenti del responsabile della ditta che dovrà comunicare all'Ente eventuali cambi di ruolo degli utenti esterni autorizzati.

  Nello stesso documento sono anche riportate le regole a cui la ditta dovrà attenersi (es: garantire accesso solo da postazioni sicure, limitazioni alle operazioni da effettuare da remoto, riservatezza delle credenziali, obbligo a non usare i dati per fini diversi da quelli indicati, ecc.).

  Per ciascun utente autorizzato viene rilasciata una credenziale (certificato e password) per attivare l'accesso VPN.

4.4 Gestione delle credenziali

Ogni credenziale di identificazione informatica E' NOMINATIVA E PERSONALE. Non è consentito l'utilizzo della stessa credenziale da parte di più utenti.

Le credenziali non nominative possono esistere solo per esigenze tecniche molto specifiche (es: servizi di emergenza, accesso ad informazioni da parte di software installato sui server) non risolvibili con altri strumenti e devono comunque essere attuate politiche per ridurre gli eventuali rischi di violazione. Ad esempio:

- privilegi minimi possibili
- attivazioni di limitazioni sui sistemi in cui possono essere utilizzate
- password molto complesse
- conservazione delle credenziali con modalità sicure

In tutti i casi è installato un modulo sul sistema di monitoraggio interno NETEYE che logga gli accessi amministrativi su Server Windows e Server Linux, Radius e database.

Ogni utente deve custodire le proprie credenziali di accesso ai sistemi, adottando le necessarie cautele per assicurare la segretezza della componente riservata e la diligente custodia dei dispositivi in proprio possesso ed uso esclusivo.

Ciascun utente è responsabile della sicurezza delle proprie password e deve adottare le necessarie cautele per mantenerle segrete. Le password sono infatti strettamente personali e non devono in nessun caso essere comunicate ad altri.

In caso di furto delle credenziali l'utente è tenuto a seguire le procedure di seguito specificate:

- in caso di furto della componente riservata (password o PIN) è necessario, al primo accesso seguente al furto, cambiare la propria password o PIN;
- darne immediata comunicazione, aprendo una chiamata di assistenza all'Help Desk o direttamente al personale preposto alle problematiche di sicurezza informatica al fine di attivare le procedure previste nel documento "GESTIONE DEGLI INCIDENTI DI SICUREZZA RELATIVI ALLA PROTEZIONE DEI DATI PERSONALI (DATA BREACH)" approvato con delibera di Giunta ID n°97 del 16/5/2019 di cui all'Allegato D_composizione gruppo di lavoro data breach.

Ciascun utente quando effettua l'accesso ad un sistema per la prima volta è tenuto a modificare e personalizzare la password di accesso che deve sottostare ai criteri di seguito identificati:

- Deve essere composta da almeno 8 caratteri
- Non deve contenere tutto o parte del nome utente
- Deve essere diversa dalla precedente
- Non deve contenere lettere accentate
- Deve rispettare almeno 2 delle 3 condizioni sotto riportate:

- Contenere una lettera maiuscola
- Contenere un simbolo (es: .;!& ……) ma non i simboli “€” (euro) e £
- *Contenere una cifra da 0 a 9*

Le politiche di sicurezza dell'Ente prevedono che la password scada ogni 90 giorni. 15 giorni prima della scadenza, ad ogni collegamento alla rete dell'Ente, viene segnalato all’utente che la password sta per scadere. L’utente è invitato a cambiarla prima dell'effettiva scadenza, seguendo la procedura allegata.
Con la password scaduta non è possibile:

- accedere alla intranet / posta dall'esterno della rete dell'Ente
- sincronizzare la posta con il telefono cellulare qualora la funzione sia abilitata.

Si raccomanda inoltre di osservare i seguenti suggerimenti per la corretta impostazione della password:

- non impostare la password in modo che sia facilmente collegabile alla propria vita privata (per es. il nome o il cognome di familiari, la targa dell’auto, la data di nascita, la città di residenza, ecc.);
- non impostare come password parole comuni riportate in un vocabolario (esistono infatti programmi fraudolenti, utilizzati per la forzatura di password che si basano su ricerche sistematiche effettuate sulle parole comuni);
- modulare il grado di complessità della password in funzione del valore dei dati e delle risorse da proteggere; password di account con privilegi amministrativi, per esempio, richiedono complessità superiori rispetto a quelle di account non privilegiati;
- scegliere password che contengono combinazioni di lettere maiuscole e minuscole, numeri, caratteri speciali (per esempio: !, *, /, ?, #);
- non utilizzare la medesima password su sistemi differenti (per es. scegliere una password di dominio differente da quella impiegata per l’accesso a siti web esterni all’Ente).
- Non scrivere la password su post-it, foglietti e altri luoghi accessibili ad altre persone.
- Non inviare le credenziali via email.
- Non rivelare le proprie credenziali a persone che si spacciano per tecnici informatici.
- Se si pensa che la password personale possa essere conosciuta da qualcuno è necessario provvedere immediatamente a cambiarla attraverso il comando CTRL+ALT+CANC – Cambia Password.
- la postazione si blocca dopo 20 minuti di inattività. Nonostante questo, se ci si assenta dall’ufficio è necessario bloccare la postazione con la sequenza di comandi ALT+CTRL+CANC per evitare che altre persone possano accedervi o utilizzare le credenziali ad insaputa dei legittimi proprietari.

La richiesta di attivazione e revoca dei servizi del sistema informativo/informatico del Comune di Reggio Emilia e l’installazione/rimozione dei pacchetti software è di competenza del Servizio Informatica.

E’ competenza del Dirigente coordinatore comunicare tempestivamente al Servizio Informatica la revoca, lo spostamento o la dismissione di un utente.
Inoltre, è ulteriore competenza del Dirigente coordinatore comunicare le applicazioni a cui l’utente deve avere accesso e le eventuali variazioni.
In caso di cessazione e/o cambio di struttura dell’utente richiedente i servizi assegnati in precedenza sono di norma revocati su istanza del Dirigente del Servizio uscente.

4.5 Disattivazione e cancellazione delle credenziali

Per “disattivazione delle credenziali” si intende il processo di inibizione dell’utilizzo delle credenziali e, conseguentemente, dell’accesso ai sistemi informatici e telematici del Comune di Reggio Emilia.

Le credenziali di autenticazione assegnate al personale, agli organismi politici ed ai soggetti esterni devono essere disattivate:

a) entro 15 giorni dall’eventuale data di interruzione del rapporto di collaborazione lavorativa con l’Ente;
b) nel caso non siano utilizzate da almeno 3 mesi, ad eccezione di quelle utilizzate per la gestione tecnica dei Sistemi Informatici e per l’accesso ai sistemi e alle basi di dati dalle applicazioni;
c) temporaneamente, in caso di necessità e di urgenza e al fine di evitare compromissioni al normale funzionamento dei sistemi o porre termine ad attività contrarie alla normativa vigente in materia di protezione dei dati personali a seguito di adozione di apposito atto da parte del dirigente competente, fino alla rimozione delle cause che hanno originato il problema.

La riattivazione delle credenziali viene eseguita dagli Account Operators su espressa richiesta:

1) dell’interessato, nei casi in cui esse siano associate a un dipendente in servizio o ad un membro degli organi politici (Sindaco, Assessori e Consiglieri comunali) che non ne abbia fatto uso per un periodo maggiore di 3 mesi;
2) del Dirigente competente nel caso di disattivazione temporanea disposta con atto del Dirigente medesimo.

Per “cancellazione delle credenziali” si intende il processo di rimozione permanente delle credenziali e dei diritti di accesso dai sistemi del Comune di Reggio Emilia e della conseguente impossibilità di utilizzo delle stesse.
La cancellazione delle credenziali è seguita anche dalla attività di cancellazione della casella di posta personale e di tutte le caselle di servizio/liste di distribuzione interne a cui l’utente faceva riferimento. La cancellazione delle credenziali deve essere effettuata:

- decorsi 3 mesi dalla disattivazione delle credenziali nei casi di interruzione del rapporto di lavoro con l’Ente di dipendenti, organi politici e soggetti esterni di cui al precedente punto a);
- decorsi 3 mesi dalla disattivazione delle credenziali nei casi in cui il soggetto titolare

delle stesse sia deceduto o ne sia stata dichiarata la morte presunta di cui al precedente punto b);
- decorsi 3 mesi dalla disattivazione delle credenziali per inutilizzo o per sospensione di cui ai precedenti punti c),
- nel caso di mancata riattivazione.

La cancellazione rende impossibile il processo di riattivazione ed obbliga la riemissione di nuove credenziali e reimpostazione dei diritti di accesso.

4.6 Autorizzazione a risorse informatiche

La concessione del diritto di un soggetto incaricato al trattamento ad accedere a una o a più risorse informatiche dell'Ente deve essere richiesta dal Dirigente competente.
L'accesso alle risorse informatiche del Comune di Reggio Emilia è consentito agli utenti abilitati in relazione al ruolo ricoperto, per il solo periodo di durata del rapporto con l'Ente e non oltre i termini di disattivazione delle credenziali.
Nel caso di cessazione del diritto di un incaricato ad accedere a una o a più risorse informatiche del Comune di Reggio Emilia è onere del Dirigente competente assicurarsi, presso il servizio Help Desk del Servizio Informatica, dell'avvenuta disattivazione delle autorizzazioni associate a tale incaricato.

4.7 Utilizzo dei dischi di rete

Ogni utente ha a disposizione i seguenti dischi di rete:

Lettera Unità	Finalità	Quota
W:	Per documenti riservati del singolo utente. E' visibile solo all'utente stesso; i documenti non sono accessibili in caso di assenza. Non dovrebbe contenere documenti di lavoro del servizio o accessibili ad altri gruppi di utenti. Per questa tipologia di documenti usare il disco I: richiedendo eventualmente la creazione di cartelle con diritti personalizzati come indicato nel par. 3.4	1 GB
H:	Applicazioni di rete	---
M:	Utilizzo trasversale tra servizi: cartelle a cui possono accedere persone appartenenti a più servizi	---
U:	Necessario per poter eseguire applicazioni Oracle	---
X:	Necessario per poter eseguire applicazioni Oracle	---
Y:	Disco di scambio visibile a tutto l'ente. NON DEVE CONTENERE DATI RISERVATI, PERSONALI E CATEGORIE PARTICOLARI DI DATI PERSONALI AI SENSI DEL REGOLAMENTO UE 2016/679"	---
I:	Disco dei singoli servizi. Contiene generalmente una cartella	Dipende

	"Documenti Servizio" accessibile a tutti i membri del servizio e una per ciascuna UOC. E' possibile richiedere eventualmente la creazione di cartelle con diritti personalizzati come indicato nel par. 3.4, al primo livello del disco e della cartella UOC qualora siano previste dalla struttura organizzativa (ad esempio: I:\nome_cartella o I:\UOCxxxxx\ Nome_Cartella).	dal servizio
O:	Facoltativo. Disco di Archivio del servizio. Contiene materiale non più modificabile ma accessibile in lettura a tutti gli utenti del servizio	Dipende dal servizio

Se l'utente appartiene a più gruppi, come ad esempio un Dirigente con incarico su più Servizi, questo può vedere anche i dischi I:\ degli altri Servizi. In questo caso, non potendo esistere una lettera di unità uguale ad un'altra già presente, questi vengono identificati scegliendo tra P: - Q: - R: - T:

A seconda della tipologia del Servizio è possibile vedere altri dischi, utilizzando le lettere di alfabeto rimanenti, finalizzati a particolari esigenze.

Per tutti i dischi di rete di cui sopra, fatta eccezione per Y:, vengono effettuati back-up come indicato nel par.3.4.

In caso di necessità di istituire cartelle riservate sui dischi di rete e di abilitare un utente a consultare tali cartelle, la richiesta deve essere fatta dal Dirigente del Servizio competente e autorizzata dal Dirigente del Servizio informatica o suo delegato.

4.8 Disco O:

Il Disco O: è un disco di archivio ed è attivato su richiesta. La richiesta di attivazione del disco O: viene fatta dal Dirigente del servizio richiedente unitamente alla definizione delle persone indicate come "Archiviatori". Il suddetto disco è in sola lettura per tutti gli utenti del servizio che ne ha fatto richiesta ed in Scrittura per gli utenti del servizio richiedente nominati dal dirigente "Archiviatori", che hanno il compito di popolare questo disco.

Gli utenti "Archiviatori" possono però solo aggiungere contenuti e non cancellare o modificare contenuti già esistenti. E' quindi consigliato:

- progettare la struttura delle cartelle "a tavolino" condividendola con i colleghi del servizio ed analizzando le varie esigenze;
- salvare in O: documenti che di solito non vengono modificati (ad esempio progetti già chiusi, immagini, ecc.);
- non salvare sul disco O: documenti intermedi (ad esempio varie revisioni, documenti di lavoro del progetto, ecc.) E' quindi necessario procedere ad una attività di "pulizia" dei contenuti da archiviare;

- creare la struttura delle cartelle/documenti che si vogliono aggiungere su I: e, una volta completata, spostarla su O:

I documenti archiviati su O: devono essere cancellati da I:

Il disco O: è presente tra i dischi di rete dei soli Servizi che ne hanno fatto richiesta.

Ogni utente, anche in caso possa accedere a dischi I: di Servizi diversi, può vedere solo il disco O: relativo al Servizio cui e' assegnato.

La cancellazione dei dati all'interno dei Dischi O: dell'Ente è operazione esclusiva degli Amministratori di Sistema.

Per richiedere la creazione del disco O:, il Servizio richiedente deve inviare una mail al Dirigente del Servizio Informatica indicando:

- Finalità
- Utenti Archiviatori

4.8 Regole sulle quote

Con "quota" si intende lo spazio massimo utilizzabile per ogni risorsa.

Le quote vengono definite dagli Amministratori di Sistema e servono per gestire correttamente lo spazio impedendo che l'uso eccessivo di spazio da parte di un Servizio possa penalizzarne altri.

Esistono 2 tipologie di quota:

- **Softquota** (soglia di guardia): Viene inviata giornalmente una mail di notifica dell'imminente raggiungimento della quota in cui viene riportata la % di riempimento. Per I: e per O: la mail viene inviata alla casella di posta del Servizio e tutti gli utenti sono invitati a controllare il contenuto del disco di rete, cancellando quanto non serve e/o chiedendo al collega "archiviatore" lo spostamento sul disco O:, se attivato. Per W: la mail viene inviata alla casella personale nominativa. Il disco rimane comunque accessibile in scrittura fino al raggiungimento dell'HardQuota.
- **HardQuota** (soglia limite): Viene inviata una mail di notifica alla casella del servizio/personale indicante il blocco completo in scrittura del disco I, O o W:.

4.9 Accesso a servizi applicativi da internet

Diversi servizi applicativi erogati dall'Ente sono accessibili da internet previo meccanismo di autentica che determina i ruoli all'interno dell'applicazione stessa. I servizi accessibili sono elencati nell' "Allegato C_Risorse accessibili dall'Esterno".
I soggetti accreditati al dominio del Comune di Reggio Emilia possono aver accesso ai servizi del Comune di Reggio Emilia (a seconda dei ruoli/privilegi assegnati) ed esposti sulla rete

esterna o resi disponibili in modalità cloud, pertanto fruibili attraverso una pluralità di dispositivi.
Le modalità di rilascio delle credenziali per le varie tipologie di utenti (dipendenti, incaricati esterni, dipendenti di altri enti, ecc.) sono descritte nella sezione 4.
Al fine di mantenere la sicurezza dei dati di proprietà dell'Ente trattati attraverso tali dispositivi, è necessario che l'utente adotti gli accorgimenti e gli strumenti necessari per garantire la riservatezza, l'integrità e la disponibilità dei dati memorizzati sull'infrastruttura informatica del Comune di Reggio Emilia, prevenendone la memorizzazione insicura ovvero la loro trasmissione attraverso una rete insicura, dove possono essere facilmente compromessi.
Si sottolinea quindi nuovamente l'importanza della corretta gestione delle credenziali, soprattutto qualora permettano l'accesso a sistemi con dati particolari accessibili da Internet.

Tecnicamente l'Ente ha adottato soluzioni per prevenire il furto dei dati come ad esempio l'utilizzo di protocolli (vedi: HTTPS, SSH, ecc.) cifrati per lo scambio delle informazioni.

In alcune applicazioni, come Jente_Finanziaria, è prevista la firma remota dei mandati di pagamento attivabile tramite l'uso di un codice che cambia ad ogni transazione in aggiunta alla password nominativa. Tale codice (One Time Password) viene inviato su un dispositivo mobile assegnato a ciascun utente abilitato.

Nel caso di accesso a sistemi software che richiedano un'autenticazione personale tramite SPID (sistema pubblico di identità digitale), l'utente è tenuto ad utilizzare la propria identità personale SPID (che gli potrà essere rilasciata gratuitamente tramite gli uffici RAO di LepidaID).

Per registrarsi a SPID l'utente deve fornire un numero di cellulare (privato o assegnatogli dall'Ente), che viene poi utilizzato successivamente per inviare un codice diverso per ogni tentativo di accesso. Questo rende più sicuro il logon in quanto abilita un'autenticazione detta a due fattori. In tutti i casi l'obiettivo di queste disposizioni è la tutela dell'utente stesso che, adottando i comportamenti indicati, non incorre in violazioni delle normative vigenti.

5. Utilizzo di postazioni di lavoro portatili (notebook) forniti dall'Ente

Se la dotazione fornita dal Comune di Reggio Emilia prevede l'utilizzo di computer portatili occorre adottare comportamenti adeguati a prevenire l'accesso da parte di soggetti non autorizzati in ragione della:

- natura dei dispositivi: tali dispositivi sono facilmente trasportabili ed occultabili;
- natura dei dati presenti sui dispositivi mobili: possono essere presenti copie parziali e/ o temporanee di dati personali o comunque di importanza strategica per la sicurezza dei sistemi;
- modalità di utilizzo dei dispositivi: possono essere utilizzati in contesti diversi anche al

di fuori di sedi dell'Ente ed in aree non sicure e ciò rappresenta una minaccia per la sicurezza dei sistemi nel momento in cui ci si riconnette alla rete interna.

Il Dirigente del Servizio richiedente dovrà effettuare richiesta scritta adeguatamente motivata al Dirigente del Servizio Informatica. La richiesta dovrà comunque essere autorizzata dal Dirigente del Servizio Informatica previe verifiche tecniche ed economiche.
Il portatile può essere richiesto per un singolo utente o ad uso del Servizio.
Nel secondo caso deve essere comunque identificato, da parte del Dirigente competente, un dipendente responsabile del corretto utilizzo del dispositivo e che si occupi del suo collegamento in rete almeno settimanalmente. Questa operazione è indispensabile per il mantenimento del dispositivo all'interno dei sistemi di gestione centralizzata dell'Ente e per la ricezione degli aggiornamenti di sicurezza.

Qualora il dispositivo non venga gestito correttamente (es: danneggiamenti, manomissioni, abbandono) o non venga collegato alla rete, il Servizio Informatica provvederà al ritiro.

5.1 Prevenzione

Per quanto sopra precisato è fatto divieto ad ogni utente di salvare in locale credenziali che consentano l'accesso alla rete o ad applicazioni del Comune di Reggio Emilia.
Al fine di evitare accessi non autorizzati ai dati e ai Servizi del Comune di Reggio Emilia si raccomanda di:

- provvedere, al momento della riconnessione alla rete interna del Comune di Reggio Emilia, al salvataggio su unità di rete o sul proprio disco personale di eventuali file copiati o creati in locale, rimuovendoli dal dispositivo mobile;
- memorizzare in forma protetta i file che contengono dati particolari così come definiti dagli Articoli 9 e 10 del Regolamento Europeo 679/2016 (ex sensibili e/o giudiziari), ad esempio proteggere i singoli documenti con password o memorizzarli in cartelle compresse (.ZIP) protette con password di cifratura.

Per prevenire furto, danneggiamento involontario e comunque situazioni di pericolo relative all'integrità dei dispositivi e dei dati, in ragione della portabilità degli stessi, l'utente è tenuto a:

- custodire adeguatamente i dispositivi durante le ore notturne o in periodi di assenza (per es. non lasciare i dispositivi sulla scrivania ma custodirli in armadi o cassetti chiusi a chiave, dotare i portatili di dispositivi di fissaggio);
- durante il trasporto osservare le istruzioni del fabbricante per la protezione dei dispositivi da urti, campi elettromagnetici e sbalzi di temperatura;
- trasportare i dispositivi come bagaglio a mano durante i viaggi in aereo;
- non lasciare i dispositivi incustoditi, neanche temporaneamente, durante i viaggi effettuati in treno o con altri mezzi di trasporto;

- non lasciare i dispositivi in auto, se non in casi eccezionali, e comunque chiuderli nel bagagliaio non a vista in modo da non evidenziarne la presenza dall'esterno;
- non lasciare i dispositivi in vista nelle stanze degli hotel, ma chiuderli in un armadio o in una valigia o depositarli in cassaforte se si prevede un'assenza prolungata.

I computer portatili ad uso individuale devono essere utilizzati esclusivamente dall'utente a cui gli stessi sono stati assegnati.
Gli utenti assegnatari provvedono al collegamento delle postazioni di lavoro portatili alla rete del Comune di Reggio Emilia almeno una volta ogni 7 giorni per effettuare gli aggiornamenti automatici del software antivirus e delle patch di sicurezza del sistema operativo e di tutti i prodotti software installati.
L'antivirus Kaspersky, installato su ogni postazione di lavoro, e' comunque configurato in modo da scaricare le firme ed altri informazioni per l'individuazione di agenti malevoli appena il dispositivo stesso viene connesso ad internet, anche al di fuori della rete dell'Ente.
Se l'utente assegnatario utilizza il dispositivo mobile per telelavoro, è comunque tenuto ad osservare le disposizioni illustrate nel paragrafo relativo, pena il ritiro dello stesso.
Qualora, per necessità particolari, sia installato il software per l'accesso VPN l'utente è obbligato ad utilizzare questo tipo di accesso ESCLUSIVAMENTE sul portatile su cui e' stato configurato e solo per le finalità indicate nella richiesta.

5.2 Dispositivi smartphone e tablet forniti dall'Ente

I dispositivi mobili, in ragione della loro natura, rappresentano una minaccia rilevante alla confidenzialità dei dati e delle informazioni del Comune di Reggio Emilia. Specificatamente i dispositivi mobili sono soggetti a rischi specifici quali perdita di informazioni, accesso a dati personali e particolari, facilità di furto, accesso a reti wireless non sicure, possibilità di download di app con contenuto malevolo.
La gestione dei dispositivi mobili assegnati dal Comune di Reggio Emilia a dipendenti e organi politici avviene attraverso una procedura che ha lo scopo di monitorare la sicurezza di tali dispositivi.
Per ridurre il livello di esposizione alle minacce viene stabilito che:

- Ogni utente che riceve in dotazione un dispositivo mobile è responsabile del suo corretto utilizzo;
- Ogni utente deve attivare l'impostazione del blocco dello schermo dopo pochi minuti di inattività (interazione utente - device) con sblocco attraverso password, pin o riconoscimento biometrico;
- È fatto divieto all'utente di installare software che comportino rischi per la sicurezza e di modificare funzionalità del sistema operativo del dispositivo mobile attraverso operazioni di "rooting" o "jailbreaking" *(vedi glossario per il significato dei termini)*;
- Evitare di salvare sul dispositivo documenti con dati personali e particolari. Se è indispensabile farlo, provvedere alla rimozione appena possibile.
- Al fine di evitare il furto dei dispositivi, con conseguente pericolo di accesso ai dati contenuti all'interno, l'utente è tenuto a non lasciare incustodito il dispositivo mobile, sia all'interno che all'esterno degli uffici dell'ente, riponendolo in cassetti o armadi

chiusi a chiave in caso di non utilizzo;
- In caso di furto o smarrimento del dispositivo, l'utente è tenuto a segnalarlo tempestivamente al Servizio che gestisce il dispositivo, in modo che gli incaricati della gestione dei dispositivi mobili del Comune di Reggio Emilia provvedano, se possibile, alla cancellazione remota dei dati contenuti all'interno ("remote wiping");
- L'utente deve inoltre informare tempestivamente il Servizio Informatica dell'avvenuto furto e procedere con regolare denuncia presso le autorità competenti.

Le regole di cui sopra valgono anche per i tablet in dotazione alla Polizia Municipale con le seguenti particolarità:

- il dispositivo è in carico al Servizio PM ed assegnato a rotazione all'agente limitatamente al suo turno di servizio.
- La configurazione è definita dal Servizio Informatica in accordo con il Dirigente della PM e l'utente non può cambiarla ne' installare app aggiuntive.

Attualmente le configurazioni di cui sopra sono effettuate manualmente dal personale incaricato del Servizio Informatica.

5.3 Telelavoro

Ai collaboratori dell'Ente con rapporto di lavoro a distanza viene consegnata una postazione di lavoro ed una linea dati ed un telefono: l'utente può quindi accedere, anche dalla propria abitazione (direttamente o tramite VPN), a tutti i dati e servizi a cui accede normalmente in ufficio.
La postazione di telelavoro è installata, configurata e mantenuta dal Servizio Informatica.
L'utente in telelavoro è tenuto a:

- utilizzare la postazione di lavoro fornitagli esclusivamente per motivi inerenti l'attività lavorativa;
- rispettare le norme di sicurezza indicate nel presente disciplinare;
- non manomettere in alcun modo gli apparati e l'impianto generale;
- non variare la configurazione della postazione di telelavoro;
- non sostituirla con altre apparecchiature o dispositivi tecnologici. Per evidenti ragioni di sicurezza tale postazione non può essere impiegata con collegamenti alternativi o complementari a quello installato/autorizzato dall'Ente ed il suo utilizzo non può essere consentito ad altri soggetti all'infuori del telelavoratore.

5.4 Utilizzo di smartphone e tablet personali per l'accesso a dati e servizi dell'Ente

E' possibile accedere a servizi erogati dal Comune di Reggio Emilia da Internet e quindi anche a mezzo di smartphone e tablet anche di proprietà personale, sia nel caso in cui la SIM card sia di proprietà personale, sia nel caso in cui la SIM card sia fornita dal Comune di Reggio Emilia.

Inoltre è possibile configurare l'accesso alla propria casella di posta e alla propria agenda di lavoro sul proprio telefono personale. Il Servizio Informatica fornisce indicazioni su come configurare l'accesso, ma non interviene in nessun modo su dispositivi non di proprietà dell'Ente.
Il personale del Servizio Informatica è autorizzato ad effettuare il passaggio dei dati tra dispositivi mobili di proprietà dell'Ente.
In caso si ravvisi la necessità di effettuare passaggi dati su dispositivi non di proprietà dell'Ente, tale passaggio è richiesto dal Dirigente del Servizio competente e consentito solo ed esclusivamente su sim aziendali. L'uso dei dispositivi personali su cui sono installate sim aziendali è di esclusiva responsabilità del proprietario del dispositivo e l'Ente è sollevato da ogni responsabilità giuridica connessa.

Per questi casi, oltre a quanto già prescritto nel paragrafo precedente, si stabilisce che:

- I protocolli consentiti per l'accesso alla posta elettronica da smartphone e tablet sono: Activesync via App Gmail su Account Exchange.
- La configurazione dell'account aziendale sull'app nativa per la gestione della posta elettronica è subordinata, per funzionare, all'applicazione della procedura di configurazione manuale indicata dal Servizio Informatica e che l'utente deve eseguire autonomamente. Il servizio informatica non garantisce il funzionamento su dispositivi personali.
- L'utente è tenuto ad impostare il blocco automatico dello schermo dopo pochi minuti di inattività con sblocco attraverso password, pin o riconoscimento biometrico.
- Al fine di evitare il furto dei dispositivi, con conseguente pericolo di accesso ai dati contenuti all'interno, l'utente è tenuto a non lasciare incustodito il dispositivo mobile.
- L'utente deve inoltre informare tempestivamente il Servizio Informatica dell'avvenuto furto e procedere con regolare denuncia presso le autorità competenti.
- Nel caso in cui l'utente sospetti una violazione dei dati del Comune di Reggio Emilia, la presenza di un malware, oppure la compromissione del proprio dispositivo mobile personale utilizzato per accedere ai dati del Comune di Reggio Emilia, è tenuto a segnalarlo tempestivamente al Servizio Informatica, in modo che, se fosse confermata una compromissione di dati, possano essere attivate opportune contromisure al fine di limitare i danni.

6. Utilizzi della rete del Comune di Reggio Emilia

Al fine di prevenire l'accesso ai sistemi informatici da parte di soggetti non autorizzati è fatto divieto di:

- connettere ad Internet, tramite reti wifi, modem o altri apparati di accesso remoto non espressamente autorizzati, strumentazioni informatiche collegate alla rete interna del Comune di Reggio Emilia;
- connettere alla rete interna del Comune di Reggio Emilia strumenti elettronici personali o comunque non espressamente autorizzati;
- connettere alla rete interna del Comune di Reggio Emilia access point o altri apparati di rete non espressamente autorizzati;
- installare e/o comunque utilizzare software peer-to-peer o utilizzare le postazioni di lavoro collegandole tra loro per la condivisione di file e stampanti;
- utilizzare strumenti di cattura, analisi del traffico di rete o sfruttare vulnerabilità nei sistemi
- utilizzare strumenti/metodi per sbloccare/utilizzare software protetto da licenza;
- diffondere volontariamente programmi nocivi (per es. virus, worm, spyware, ecc.) nella rete o nei sistemi.

È attivo un sistema di Network Access Control (NAC) che permette l'autenticazione sulla presa di rete solo se:

- la postazione windows è autorizzata
- se al log-on vengono inserite credenziali valide.

Nel caso in cui le due condizioni di cui sopra non siano entrambe soddisfatte, il dispositivo viene rediretto su una rete che ne permette la sola navigazione Internet ed esclude l'accesso alla rete interna dell'Ente. In questo caso l'accesso ad internet avviene senza nessuna limitazione (vedi regole per la navigazione internet alla sezione 8), ma vengono mantenuti i log della navigazione come indicato nella sezione 10. Le stesse regole sono applicate alla rete WIFI dell'Ente, per tablet e smatphone.

7. Posta elettronica

La casella di posta elettronica viene fornita dal Comune di Reggio Emilia quale strumento di supporto per lo svolgimento dell'attività lavorativa e delle attività che siano strumentali e connesse alla stessa.
Le caselle di posta elettronica sono assegnate come servizio di base a ciascun dipendente e membro degli organi politici al momento dell'inquadramento giuridico.
Agli incaricati esterni accreditati al dominio del Comune di Reggio Emilia la casella di posta è assegnata, su richiesta motivata del Dirigente richiedente. La richiesta di attivazione dei servizi di posta personale del Comune di Reggio Emilia agli incaricati esterni accreditati, segue le procedure di attivazione precedentemente descritte.
L'attivazione di ulteriori caselle di posta elettronica, per attività di gruppo o di progetto, può essere richiesta al Dirigente del Servizio Informatica o suo delegato dal Dirigente del servizio richiedente con le procedure di attivazione precedentemente descritte.

Il combinato disposto dell'Articolo 15 della Costituzione e delle norme a tutela dei dati personali contenute nel Regolamento europeo 679/2016 impongono impostare alcune regole del gestionale di posta elettronica in dotazione all'Ente:

- è fatto divieto ed è inibito di default di reindirizzare in modo automatico ad altro soggetto interno o esterno all'Ente le mail ricevute in quanto la corrispondenza che il mittente intende indirizzare ad un determinato soggetto verrebbe vista anche da altri.
- è possibile utilizzare gruppi di posta di ufficio (es. ufficioxxxxxx@comune.re.it) in modo tale che il mittente sia cosciente che sta scrivendo ad una pluralità di interlocutori e non ad una specifica persona.
- non è ammissibile la pratica di autorizzare la condivisione della propria casella di posta nominativa (nome.cognome@comune.re.it) ad altri dipendenti.
- È autorizzata la condivisione dell'agenda del sistema di posta dell'Ente con altri soggetti, con la raccomandazione di indicare come PRIVATI eventuali appuntamenti contenenti dati personali.

Le caselle di posta elettronica certificata (PEC) non sono di norma nominative, ma sono d'ufficio o di procedura ad eccezione di quelle del SERVIZIO LEGALE per ragioni imprescindibili di ufficio. Le caselle PEC d'ufficio o di procedura sono assegnate ai Servizi dell'Ente per le quali sono previsti processi di comunicazione istituzionale con soggetti terzi. L'attivazione di nuove caselle PEC può essere richieste dal Dirigente competente al Responsabile della gestione documentale dell'Ente e segue le procedure di attivazione descritte nel "Manuale di gestione del protocollo informatico, dei flussi documentali e degli archivi" adottato dall'Ente con delibera di giunta ID.140 del 28 Luglio 2016.

Al fine di assicurare la disponibilità dei dati e delle informazioni pervenute o inviate dalle caselle di posta elettronica si raccomanda la creazione e l'utilizzo di caselle di posta

elettronica di struttura e/o di progetto condivise tra gli utenti che concorrono alle suddette attività.
La gestione degli utenti che accedono a caselle di struttura, di gruppo o di progetto è assegnata dagli Amministratori di sistema nominati dal Servizio Informatica.
Nei casi in cui siano utilizzati quali mezzi per trasmettere dati personali a soggetti terzi, si rammenta che tale operazione costituisce comunicazione di dati personali e, come tale, deve essere effettuata nel rispetto delle misure di sicurezza previste dall'Articolo 32 del Regolamento Europeo 679/2016.
L'accesso al contenuto della casella di posta elettronica personale è consentito solo all'utente assegnatario. L'accesso da parte di terzi alla casella personale di un utente è vietato.

7.1 Utilizzo della Posta Elettronica

La posta elettronica deve essere utilizzata esclusivamente per le specifiche finalità della propria attività lavorativa, nel rispetto delle esigenze di funzionalità e sicurezza dei sistemi informativi e degli altri utenti del Comune di Reggio Emilia e dei processi lavorativi, adottando comportamenti idonei a prevenire la perdita di confidenzialità di dati riservati e l'utilizzo non appropriato di beni del Comune di Reggio Emilia.

7.2 Quote della Posta Elettronica

Nell'infrastruttura di posta sono presenti 6 tipologie di quota a seconda del tipo di casella (Utente/Servizio).
Ogni nuova casella, sia essa di servizio o utente, inizialmente ha 1Gb di quota; non possono esistere caselle email senza limite di quota.
Le quote disponibili sul sistema di posta sono: 1-2-3-4-6Gb.
Aumenti TEMPORANEI di quota vengono concessi dal Dirigente del Servizio informatica o suo delegato solo in casi eccezionali e debitamente motivati. In ogni caso, al raggiungimento della quota prevista, per ogni casella è obbligatorio il contenimento dello spazio occupato applicando la procedura di archiviazione a carico dell'utente.
L'utente è costantemente informato sullo stato della quota da una barra di avanzamento presente nella parte superiore destra della casella di posta.
Al raggiungimento dell'85% della quota, e fino a quando la barra non scende da questo valore, l'utente riceve giornalmente una mail che lo informa del prossimo raggiungimento del 100% della quota.
Una volta raggiunto il 100% della quota, la casella viene chiusa e non riceve più posta, ne dall'interno, ne dall'esterno.

7.3 Archiviazione della Posta Elettronica

Ogni utente ha il dovere di tener manutenuta la propria casella di posta elettronica personale. Sulla Intranet sono presenti i manuali per effettuare l'archiviazione degli allegati liberando così spazio sulla casella di posta, pur mantenendo i messaggi originali da cui sono stati rimossi gli allegati.

Gli Amministratori di Sistema controllano giornalmente lo stato delle caselle di servizio, e quando queste arrivano al 95% della quota, effettuano l'archiviazione degli allegati sul disco I del settore in cartelle che ne identificano la tipologia, ad es:

I:\Officedoc\BKUPCaselladiServizio

L'archiviazione delle caselle di servizio viene effettuata in autonomia dagli Amministratori di Sistema senza informare l'utente.

In qualsiasi caso, gli allegati estratti non sono più presenti all'interno dell'infrastruttura di posta, quindi non possono essere ripristinati.
E obbligo dell'utente di tutelare, copiandoli ad esempio su CD o su Memorie esterne i propri archivi di posta personali. Il Servizio Informatica non è responsabile della perdita dell'archivio personale.

Gli archivi delle caselle di servizio, essendo copiati su dischi I, sono sottoposti a backup giornaliero e recuperabili in caso di cancellazione involontaria.

7.4 Regole per la gestione dello Spam

"Spam" è il termine con cui si indica l'invio incessante, ma soprattutto indesiderato di messaggi pubblicitari o parti delle cosiddette catene di S. Antonio ad un gran numero di utenti contemporaneamente.
Il sistema di posta dell'Ente ha integrato un software Antispam.
Il sistema Antispam installato potrebbe generare falsi positivi è quindi necessario integrare le misure di sicurezza con informazioni aggiuntive da fornire agli utenti.
In questi casi occorre seguire le seguenti regole:

- Se l'utente è in attesa di una mail e non la vede comparire nella postia in entrata, deve verificare nella cartella "Posta indesiderata" e trascinarla in POSTA IN ENTRATA.
- Se l'utente riceve nella casella di posta in entrata messaggi pubblicitari o altre mail che rientrano nella categoria "SPAM", deve selezionarle e trascinarle in POSTA INDESIDERATA.

In entrambi i casi il sistema "impara" e la volta successiva gestirà correttamente quel tipo di mail sia per gli utenti che per i mittenti.

Per ridurre il rischio di finire in liste di spammer si raccomanda di:

- non rispondere mai a messaggi di presunto spamming, neppure se al momento della cancellazione della mail viene richiesta conferma di lettura dal mittente, poiché ciò consente al mittente di verificare l'effettiva esistenza dell'indirizzo di posta dell'utente;
- limitare al minimo indispensabile la diffusione del proprio indirizzo di e-mail su siti web pubblici (per es. forum, mailing list, ecc.);
- non rispondere o inoltrare email di c.d. "Catene di S. Antonio", ovvero messaggi dal

contenuto ambiguo che esortano ad inoltrare urgentemente delle copie ad altre persone;
- non configurare la conferma di lettura in modalità automatica.

7.5 Suggerimenti per la prevenzione da malware

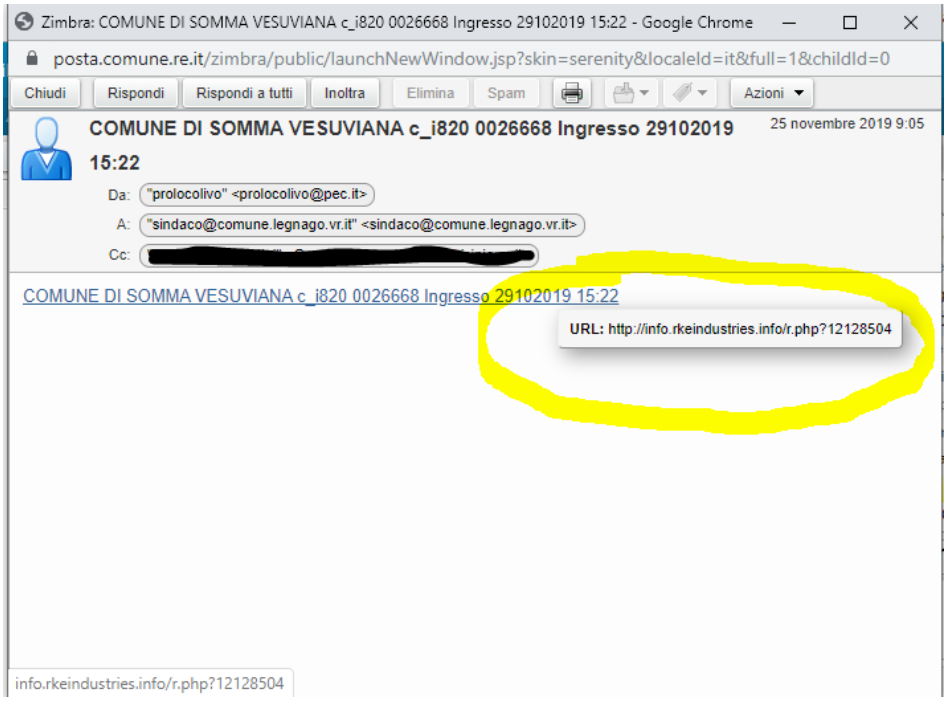
La maggior parte degli attacchi informatici viene veicolata tramite la posta elettronica. E' quindi fondamentale essere attenti nella gestione delle mail in arrivo.
Il phishing è una tecnica di attacco molto utilizzata che sfrutta email e siti web "fantasma", del tutto simili nell'aspetto agli originali, per ingannare l'utente e carpire informazioni confidenziali o personali. Questo viene fatto tipicamente chiedendo di scaricare allegati o di connettersi a siti web che sembrano essere autentici, ma in realtà non lo sono.
È necessario prestare massima attenzione alle email che richiedono di fornire dati riservati quali password o numeri di carta di credito, attraverso la compilazione di moduli web (per es. da parte di una banca, di un operatore telefonico, di studi legali o di fornitori di servizi quali Yahoo!, Postecom, ecc.).
Le modalità con cui gli hacker costruiscono le campagne di phishing cambiano, ma i principali accorgimenti da tenere presente per capire se una mail può essere pericolosa sono i seguenti:

- Controllare il mittente, ad esempio nel seguente caso non è chi dice di essere:

```
Da: "Ufficio Traffico <ufficio.traffico@comune.re.it>" <dsandoval@rafman.mx>
A: "Nome Cognome" <Nome.Cognome@municipio.re.it>
Inviato: Lunedì, 21 ottobre 2019 12:03:59
Oggetto: reclamo - Ufficio Traffico
```

Evidenziato in giallo, il mittente VERO della mail di cui sopra.

- controllare l’url se e’ nascosto, ad es



- fare attenzione a testi grammaticalmente scorretti
- diffidare dei messaggi che richiedono azioni da fare con urgenza
- non inserire mai le proprie credenziali

A fine di prevenire le minacce rappresentate da software malevoli (per es. virus, worm, spyware, ransomware ecc.) che potrebbero essere contenuti in email o negli allegati delle email stesse, si forniscono le seguenti indicazioni:

1. Non scaricare allegati di posta da mail che provengono da mittenti non conosciuti
2. Non inserire mai le proprie credenziali in pagine i cui link vi arrivano via email.
3. In caso di campagne di phishing, mail malevole arrivano spesso contemparaneamente a più persone: chiedete ai colleghi se hanno ricevuto mail simili.
4. Controllate la bacheca intranet: in caso di campagne di phishing o di altri attacchi, come indicato sotto, vengono pubblicate indicazioni specifiche sulle attenzioni/operazioni da fare.
5. In caso di dubbi sulla qualità di messaggi email, si raccomanda di contattare l'indirizzo di posta dedicato alle problematiche di sicurezza informatica del Comune di Reggio Emilia:
   segnalazioni.spam@comune.re.it

Ogni volta che si presenta una potenziale minaccia il Servizio Informatica adotta

tempestivamente le seguenti misure:

1. Nell'immediato, per evitare il propagarsi dell'incidente, si procede a resettare le password delle credenziali degli utenti potenzialmente compromessi.
2. Si pubblica un messaggio in bacheca per avvisare gli utenti della pericolosità del Phishing/Virus/Malware.
3. In caso di sospetto di compromissione dei dati personali si adottano le procedure previste dal documento: "GESTIONE DEGLI INCIDENTI DI SICUREZZA RELATIVI ALLA PROTEZIONE DEI DATI PERSONALI (DATA BREACH)" approvato con delibera di Giunta ID 97 del 16/5/2019.
4. Modifica della configurazione del firewall per bloccare l'accesso al sito.
5. In casi di particolare gravità si procede a resettare le password di tutti i dipendenti dell'Ente.

7.6 Recupero di Mail da parte del Comune di Reggio Emilia in assenza dell'utente

In caso di necessità di recupero di mail da parte del Comune di Reggio Emilia su una casella di posta personale in assenza del dipendente titolare (ferie, dimissioni, pensionamento), gli Amministratori di sistema del Servizio Informatica, a seguito di autorizzazione scritta (inviata da mail personale non dell'Ente) da parte del proprietario della casella, procedono al recupero della mail, fermo restando che la casella di posta sia ancora disponibile e non sia stata già cancellata.

8. Navigazione in internet

Il Comune di Reggio Emilia fornisce l'accesso a Internet a supporto dello svolgimento dell'attività lavorativa e delle attività che siano strumentali e connesse alla stessa e per questo se ne prescrive un utilizzo pertinente alle specifiche finalità, nel rispetto delle esigenze di funzionalità e di sicurezza della rete e dei sistemi.
È fatto divieto di:

- scaricare o eseguire alcun software o altro contenuto attivo, anche se gratuito, da siti Internet se non per finalità istituzionali e solo se strettamente necessario. In tal caso, verificare la provenienza e l'autenticità del software (per es. tramite meccanismi di firma digitale);

- utilizzare siti pubblici di condivisione dei file e di archiviazione online forniti da provider che non assicurano strumenti di protezione adeguati. Il Servizio Informatica ha attivato un sistema di File Sharing Interno denominato Sharebox (https://sharebox.comune.re.it/) che permette di rendere disponibile a soggetti esterni all'ente file di grandi dimensioni (fino a 50 Mb). Tale sistema funziona in modo similare a WeTransfer e consente di caricare il file da rendere disponibile e di ottenere un link e una password da inviare alla persona che dovrà scaricarlo. In questo modo non si sovraccarica inutilmente la casella di posta e non si supera il limite del 15 MB per gli allegati della email. Il file reso disponibile all'esterno rimane sui server dell'Ente e non in cloud, ciò ai fini della protezione dei dati personali ivi contenuti. Per usufruire di questo strumento occorre essere abilitati. Pertanto chi ha necessità di utilizzarlo deve fare richiesta di abilitazione aprendo un ticket di "assistenzainformatica".

- caricare documenti inerenti l'attività lavorativa o istituzionale, soprattutto se contenenti dati personali, di particolari categorie e/o relativi a condanne penali e reati, su siti pubblici di condivisione, archiviazione o backup online.

Per contrastare le nuove tipologie di attacco informatico che hanno come obiettivo l'utente finale e come mezzo di propagazione il web o la posta elettronica e le comunicazioni web che utilizzano sempre più frequentemente canali cifrati, il personale del Servizio Informatica addetto alla sicurezza informatica è autorizzato a configurare sistemi di sicurezza dedicati alla navigazione web, per ispezionare il traffico cifrato nei siti ritenuti ad alto rischio (tipicamente quelli che permettono lo scambio di documenti) allo scopo di individuare e bloccare eventuale malware o strumenti di attacco. Tale ispezione, funzionale unicamente alla verifica della sicurezza delle informazioni, è effettuata con strumenti automatici; per nessun motivo viene utilizzata per il controllo dell'attività lavorativa.

In particolare è attivo lo strumento di URL filterig che tramite meccanismi centralizzati di classificazione dei siti o di parte di essi definisce delle categorie su cui sono state impostate regole di accesso.

Le principali regole impostate dal Servizio Informatica sono:

- Blocco dei siti appartenenti a categorie pericolose per la sicurezza dei sistemi o sicuramente non coerenti con l'attività lavorativa. Alcune di queste categorie sono: Games, Hacking, Violence, Sex, Spyware/Malicious Sites, ecc.
  Qualora il sito a cui si deve accedere sia legittimo e risulti invece categorizzato male e quindi non accessibile, si può richiedere la verifica cliccando sulla voce opportuna della pagina in cui compare il divieto di accesso. La verifica della catalogazione richiede qualche giorno perché non viene fatta dal personale del Servizio Informatica. In casi urgenti si può aprire un ticket di assistenza per consentire l'accesso in attesa della catalogazione corretta. Alcuni siti potrebbero essere necessari per l'attività lavorativa sopratutto di alcuni Uffici dell'Ente, anche se la categoria sarebbe tendenzialmente non inerente l'attività lavorativa. Alcune possibili categorie sono: Sport, Travel, Social Network, shopping, News/Media, ecc. Quando si accede a siti compresi in queste categorie compare una pagina in cui l'utente viene avvisato che il sito potrebbe non essere inerente l'attività lavorativa ed è sua responsabilità dichiararne l'accesso per motivi lavorativi.
- Accesso vietato alle webmail esterne (ed esempio Gmail, Virgilio, Yahoo, ecc.): le wabmail esterne bypassano alcuni controlli di sicurezza (ad esempio verifiche su allegati) e possono incrementare il rischio di ingresso di agenti malevoli sui sistemi dell'Ente. Nel caso in cui, per ragioni di servizio, si debba utilizzare una di queste webmail il Dirigente del Servizio competente può inoltrare richiesta adeguatamente motivata al Dirigente del Servizio informatica che autorizzerà in prima persona o tramite suo delegato.
- E' bloccato l'utilizzo di strumenti di controllo remoto di terze parti. Esistono strumenti tipo teamViewer che consentono di condividere il desktop della postazione con utenti di internet. Generalmente prevedono un codice e password, generati all'inizio di ogni sezione di lavoro, che deve essere comunicato all'utente di Internet che ha richiesto la condivisione. Costituiscono comunque una vulnerabilità in termini di sicurezza perché bypassano i sistemi di controllo perimetrali e usano protocolli non ispezionabili. Questi strumenti sono utilizzati a volte da software house per fornire assistenza remota agli utilizzatori del proprio software. Queste situazioni devono essere limitate quanto più possibile, ma se necessario, il Dirigente del Servizio competente può richiedere al Dirigente del Servizio informatica lo sblocco di questo accesso per un numero RIDOTTO di colleghi. In questo caso si devono seguire le seguenti regole:
  - attivare lo strumento di controllo remoto solo per il tempo strettamente necessario;
  - essere certi della identità della persona che ha chiesto l'accesso;
  - Presidiare la postazione e controllare l'attività eseguita durante la sessione di controllo remoto;
  - Non dare mai le proprie credenziali di accesso all'applicazione o alla rete ad altri soggetti, ma inserirle direttamente quando richieste.

9. Protezione antivirus

L'utente utilizzatore delle risorse informatiche dell'Ente è tenuto ad adottare le necessarie cautele al fine di ridurre il rischio di infezione virale della propria o altrui postazione di lavoro. È fatto quindi divieto agli utilizzatori delle postazione di lavoro di rimuovere il programma antivirus installato su di essa e di alterarne la configurazione. Si invitano gli utenti a segnalare problemi eventualmente riscontrati sulla corretta installazione e funzionamento del programma antivirus installato sulla propria postazione di lavoro al Servizio Informatica del Comune di Reggio Emilia.
L'antivirus installato su tutte le Postazioni di lavoro dell'Ente procede in autonomia al controllo in automatico della presenza o meno di virus su supporti rimovibili. Ad ulteriore misura di sicurezza l'utente può, autonomamente e attraverso il menu contestuale del sistema operativo della PdL, effettuare la scansione dei dispositivi e dei file.
A seguito di segnalazione della presenza di un virus da parte del software antivirus si prescrive di non inviare ad altri utenti i messaggi di posta elettronica contenenti segnalazioni del virus. Il sistema Antivirus installato provvederà in autonomia all'eliminazione del Virus o alla messa in quarantena dello stesso. E' comunque sempre necessario informare il Servizio Informatica al verificarsi di queste evenienze.

10. Gestione dei log

I Sistemi Informativi del Comune di Reggio Emilia sono verificati, sia periodicamente sia su segnalazione di incidenti di sicurezza, allo scopo di garantirne l'efficienza, la disponibilità ed il rispetto di Leggi e Regolamenti, ed in particolare dei requisiti di sicurezza previsti dalla normativa vigente in materia di protezione dei dati personali.
Alcune attività dell'utenza sono soggette a logging: ciò significa che alcune operazioni eseguite dagli utenti di sistemi informativi vengono memorizzate in formato elettronico e conservate per un certo periodo di tempo. Il logging è necessario per ragioni di sicurezza: il livello del logging dei diversi servizi, ossia il livello di dettaglio dei dati memorizzati, è funzionale unicamente alla verifica della sicurezza con la quale i servizi sono erogati e per nessun motivo viene utilizzato per il controllo dell'attività lavorativa.

Per tutti i tipi di log le finalità della raccolta sono le seguenti:

- necessità di poter effettuare verifiche di sicurezza e poter identificare anche a posteriori incidenti di sicurezza, violazione delle policy o attività fraudolente e procedere alla raccolta delle evidenze;
- troubleshooting: indagine su problemi di funzionamento dei sistemi. In caso di malfunzionamento è spesso necessario accedere ai log per capire cosa sia successo e a volte è necessario verificare se l'anomalia si è ripetuta in passato. Quindi più è ampio il lasso temporale di raccolta e maggiore è la possibile di fare verifiche retroattive

Di seguito vengono dettagliate le tipologie di log raccolti e conservati ed eventuali finalità specifiche di ogni tipo di log:

- **log della navigazione web, del firewall e del server di posta:** scopo ulteriore della raccolta, per quel che riguarda la navigazione web, è quello di verificare il corretto utilizzo delle strumentazioni assegnate dall'Ente nello svolgimento dell'attività lavorativa;
- **log delle segnalazioni ed alert di tutte le tipologie di sistema antimalware**;
- **log degli accessi degli Amministratori di Sistema ai sistemi amministrati:** tale raccolta è motivata dalla necessità di ottemperare al Provvedimento del Garante per la Protezione dei dati personali relativo agli Amministratori di Sistema. *Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di sistema" del 27 novembre 2008;*
- **log degli accessi degli utenti ai servizi e Applicazioni di rete;**
- **log degli accessi degli utenti al sistema di stampa e delle operazioni effettuate:** scopo ulteriore della raccolta è quello di verificare il corretto utilizzo delle strumentazioni assegnate dall'Ente nello svolgimento dell'attività lavorativa;
- **log delle attività svolte da utenti e amministratori di sistema nell'ambito di alcuni software complessi:** audit sulla correttezza dei dati gestiti dal software stesso.

Tutti i log vengono conservati per 6 mesi, a meno che non sussistano rilevanti problematiche tecniche che obblighino la riduzione del periodo.

11. Prevenzione e gestione degli incidenti di sicurezza informatica

Al fine di prevenire, rilevare e rispondere efficacemente agli incidenti di sicurezza nel minor tempo possibile, è di grande rilevanza operare tempestivamente e in uno spirito di collaborazione.
Qualora si ravvisassero violazioni di sicurezza interna o eventi che possano portare a credere che vi sia stata una elusione delle misure di sicurezza previste, è necessario segnalare tempestivamente l'accaduto ai referenti del Servizio Informatica, aprendo una richiesta di assistenza all'Help Desk o comunicandolo direttamente al "Gruppo di lavoro per la gestione degli incidenti di sicurezza relativi alla protezione dei dati personali (data breach)" qualora si ravvisi il rischio di compromissione di dati personali. A tal fine si rimanda alle procedure previste dal documento "GESTIONE DEGLI INCIDENTI DI SICUREZZA RELATIVI ALLA PROTEZIONE DEI DATI PERSONALI (DATA BREACH)" approvato con delibera di Giunta ID n° 97 del 16/5/2019 e all'Allegato D_ composizione gruppo di lavoro.

In un'ottica di prevenzione degli incidenti di sicurezza, è necessario attenersi scrupolosamente alle indicazioni ricevute dal personale addetto alla sicurezza ed alla gestione della rete e dei sistemi. Tali indicazioni sono fornite agli utenti attraverso gli strumenti di comunicazione interna del Comune di Reggio Emilia.

12. Protezione dei dati trattati senza l'utilizzo di strumenti elettronici

L'accesso ai dati trattati senza l'utilizzo di strumenti elettronici è consentito, come per i trattamenti di dati personali effettuati con mezzi elettronici, esclusivamente al personale espressamente incaricato.
Vi sono, inoltre, alcuni basilari comportamenti che, se messi in atto, riducono in maniera considerevole i rischi di accesso ai dati da parte di persone non autorizzate, di perdita di confidenzialità dei dati e della conseguente mancanza di disponibilità degli stessi.
In linea con quanto sopra, è assolutamente necessario raccogliere prontamente, nel caso si utilizzino stampanti di rete o fax ubicati in locali comuni (per es. corridoi), i documenti stampati o ricevuti via fax - soprattutto se contenenti dati personali - in modo da preservarne la riservatezza del contenuto. È ugualmente rilevante, ai fini della tutela dei dati personali trattati nell'espletamento delle proprie mansioni, assicurarsi, al termine della giornata lavorativa, che i documenti contenenti dati personali o rilevanti ai fini della sicurezza del sistema informativo del Comune di Reggio Emilia, non siano lasciati a vista sulla scrivania ma conservati in cassetti o armadi. Conseguentemente e al fine di non eludere tali precauzioni, è opportuno conservare con le dovute cautele le chiavi dei cassetti e degli armadi.
E' inoltre utile prevedere la disponibilità delle stesse, durante la propria assenza dall'attività lavorativa, in modalità controllata e sicura (esempio: copia delle chiavi depositate in segreteria, registro di presa in carico e di riconsegna).
Nei casi in cui atti o documenti contengano dati di particolari categorie e/o relativi a condanne penali e reati, si raccomanda di prevedere apposita procedura per la conservazione in archivi ad accesso selezionato, disciplinando modalità di ingresso tali da consentire l'identificazione degli utenti che vi accedono. Conseguentemente si sottolinea la necessità di custodire opportunamente i documenti prelevati per impedire l'accesso improprio da parte di persone non autorizzate. In particolare, essi non dovranno rimanere incustoditi nemmeno per brevi periodi, provvedendo eventualmente a riporli in armadi o cassetti chiusi a chiave. Al termine del trattamento, l'utilizzatore avrà cura di ricollocare i documenti nell'archivio di provenienza.

13. Controlli e sanzioni

13.1 Controlli

Il Servizio Informatica o altri soggetti delegati dal Dirigente hanno facoltà di effettuare controlli, anche preventivi, sul corretto uso e funzionamento degli strumenti informatici nel rispetto dei diritti e delle libertà fondamentali dei lavoratori o dei soggetti esterni che utilizzano strumenti informatici del Comune di Reggio Emilia al fine di evitare usi impropri dei sistemi messi a disposizione dal Comune di Reggio Emilia

Possono essere effettuati controlli automatizzati sul traffico di rete volti a inibire l'accesso a siti o categorie di siti di palese natura non istituzionale.

I controlli sulle attività svolte mediante utilizzo dei sistemi informatici sono ammessi nei seguenti casi:

A. quando previsti da fonte normativa o regolamentare;
B. nel caso in cui si verifichino eventi dannosi o situazioni di pericolo non impediti da preventivi accorgimenti tecnici;
C. su segnalazione dell'Autorità Giudiziaria;
D. nel caso in cui, nell'ambito delle ordinarie attività di gestione dei sistemi informativi di competenza, siano rilevati file illegali o dal contenuto palesemente non istituzionale;

Nei casi in cui, a seguito di un controllo, si rilevino comportamenti illegali o non istituzionali, il Servizio Informatica, informato il Dirigente competente, potrà intervenire valutando se:

- inviare avvisi collettivi o individuali in cui verranno segnalati i comportamenti non corretti;
- rimuovere i file, senza alcun preavviso all'utente, nei casi in cui i file possano limitare l'utilizzo di risorse o possano recar danno all'Ente;
- inibire l'accesso a siti o categorie di siti di palese natura non istituzionale;
- informare, nei casi in cui i comportamenti non corretti si ripetano nel tempo o risultino particolarmente gravi, il Dirigente del Servizio personale, per i rispettivi ambiti di competenza, che adotteranno i provvedimenti più opportuni di cui al paragrafo successivo "sanzioni".

13.2 Sanzioni

In riferimento ai controlli e alle relative sanzioni, si rinvia a quanto previsto dall'art. 44 del vigente Regolamento sull'Ordinamento Generale degli uffici e dei servizi - Sezione C- La Gestione: "Utilizzo degli strumenti informatici in uso ai dipendenti".

I comportamenti in violazione del presente documento, aventi rilevanza disciplinare, fermi restando i diversi profili di responsabilità civile e penale, saranno sanzionati secondo le forme e le modalità previste dalle procedure interne dell'Ente.

14. Glossario

Termine/Acronimo	Descrizione
Analisi forense	insieme di tecniche rivolte all'analisi e alla soluzione dei casi legati alla criminalità informatica, comprendendo tra questi i crimini realizzati con l'uso di un computer, diretti a un computer o in cui il computer può comunque rappresentare una fonte di prova.
Autenticazione	l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità dell'utente che accede ai sistemi informativi.
Amministratori di PDL	Utenti che hanno privilegi amministrativi ma esclusivamente sulle postazioni locali
Account Operator	Utenti che hanno privilegi per gestire le credenziali di altri utenti ma non sono amministratori del dominio, ne' dei server ne' delle PDL
Black List di Reputation	Insieme di indirizzi (IP, mail) ai quali, sulla base dei comportamenti tenuti precedentemente (es. invio di spam), è impedito l'utilizzo di alcuni servizi informatici.
Cracking (strumenti di)	software che consentono l'aggiramento illecito delle misure di sicurezza di un sistema informatico.
Dati personali	qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
Dati di particolari categorie	dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona
Identificazione informatica	la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne consentono l'individuazione nei

	sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso.
Dispositivo mobile	sistema di elaborazione che può essere spostato e trasportato. Nel contesto del presente disciplinare tecnico, per dispositivo mobile si intende solo “smartphone” o “tablet”, mentre negli altri casi si parla esplicitamente di “computer portatile”, o “postazione di lavoro portatile”
Evidenza	nell’ambito dell’analisi forense, si intende una “traccia” di reato; la raccolta delle evidenze rappresenta una fase della gestione degli incidenti di sicurezza informatica, anche quando non siano presenti implicazioni legali.
Incaricato	la persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile.
jailbreaking	una procedura che rimuove le restrizioni software imposte da Apple nei propri dispositivi dispositivi e che ermette di installare software e pacchetti di terze parti, non firmati e autorizzati da Apple all’interno dell’Apple Store
Password	sequenza di caratteri alfanumerici che costituisce la chiave d'accesso ad un sistema protetto. In assenza di altri dispositivi, la password costituisce il meccanismo di sicurezza base per la protezione dell’accesso a risorse informatiche.
Patch	aggiornamento di un software per la correzione di un problema di sicurezza o di funzionalità.
Peer-to-peer (strumenti)	software che permettono l'utilizzo di una postazione di lavoro in modalità server per consentire lo scambio di file con altri utenti, anche esterni alla rete dell'Ente.
Phishing	tecnica finalizzata all'acquisizione, per scopi illegali, di dati riservati (codici di accesso, password, numeri carte di credito e altre informazioni personali) tramite l'invio di e-mail dal contenuto e dal mittente opportunamente falsificati (per es. simulando la provenienza del messaggio da parte di una banca o di uno studio legale).
Postazione di lavoro	Il pc o il portatile comprensivo di tutte le periferiche di input e output (mouse, tastiera, webcam, video, stampante collegata) che costituiscono la dotazione hardware assegnata ad un utente
Ransomware	tipo di malware che limita l'accesso del dispositivo che infetta (per esempio cifrando i dati), richiedendo un riscatto (*ransom* in

	Inglese) da pagare per rimuovere la limitazione
Responsabile del trattamento	la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.
Quota	Soglia massimo di riempimento di una risorsa (es: casella di posta, disco di rete). Si puo' differenziare in soft quota al cui raggiungimento iniziano arrivare avvisi e hard quota al cui raggiungimento è bloccata la scrittura
Rooting	processo informatico che permette agli utenti di smartphone, tablet o altri dispositivi dotati di sistema operativo Android di ottenere controlli privilegiati (conosciuti come permessi di root o amministrativi) su vari sottosistemi Android.
Scanning	attività di raccolta di informazioni su un sistema propedeutica alla fase di attacco informatico vero e proprio.
Sniffing (strumenti di)	software che consentono di intercettare ed analizzare il traffico in transito su una rete informatica.
Spamming	l'invio di grandi quantità di messaggi elettronici non richiesti (generalmente commerciali). Può essere messo in atto attraverso qualunque media, ma il più usato è Internet, attraverso l'e-mail.
Spyware	software che raccoglie informazioni riguardanti un utente senza il suo consenso, trasmettendole tramite Internet ad un'organizzazione che le utilizzerà per trarne profitto, tipicamente attraverso l'invio di pubblicità mirata.
Supporto rimovibile	dispositivo su cui è possibile registrare dati che può essere facilmente rimosso dal sistema che lo legge/scrive, trasportato in altri luoghi e collegato ad altri sistemi. Esempi di supporti rimovibili sono: chiavette USB, hard disk esterni, CD ROM.
Worm	programma in grado di autodiffondersi sulla rete e verso altri sistemi.
Virus	programma in grado di autoreplicarsi in un sistema, per esempio copiando una parte di se stesso all'interno del codice di un altro programma.
Titolare del trattamento	la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto

	dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.
Responsabile del trattamento	ogni soggetto esterno all'Amministrazione comunale che tratta dati personali per conto del Comune.
Coordinatore del trattamento	i Dirigenti dei Servizi dell'Ente individuati quali soggetti preposti a coordinare gli adempimenti necessari per la conformità dei trattamenti di dati personali, ciascuno per il proprio ambito di competenza così come definito dall'incarico dirigenziale conferito loro dal Sindaco.
Incaricato del trattamento	tutti i soggetti che effettuano operazioni di trattamento di dati personali, dipendenti e collaboratori a qualsiasi titolo e che operano sotto la diretta autorità del Titolare o dei Coordinatori.
Responsabile della protezione dei dati	figura obbligatoria prevista dagli artt. 37 e ss. del Regolamento europeo che: • informa e fornisce consulenza all'Ente in merito agli obblighi derivanti dalla normativa in materia di protezione dei dati personali; • sorveglia l'osservanza della normativa in materia di protezione dei dati personali nonché delle politiche dell'Ente in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo; • coopera con il Garante per la protezione dei dati personali; • funge da punto di contatto per l'Autorità Garante per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del Regolamento, ed effettua, se del caso, consultazioni relativamente a qualunque altra questione; • partecipa allo svolgimento delle verifiche di sicurezza svolte dal Responsabile del Servizio ICT competente o ne richiede di specifiche; • promuove la formazione di tutto il personale dell'Ente in materia di protezione dei dati personali e sicurezza informatica; • partecipa alla gestione degli incidenti di sicurezza nelle modalità previste da specifica policy dell'Ente; • formula gli indirizzi per realizzazione del Registro delle attività di trattamento di cui all'art. 30 del Regolamento. • fornisce i pareri obbligatori e facoltativi richiesti dalle strutture secondo quanto specificato di seguito.